



Configuración

SANtricity 11.6

NetApp
February 12, 2024

Tabla de contenidos

- Configuración 1
 - Alertas 1
 - Sistema: Configuración de la cabina de almacenamiento 14
 - Sistema: Configuración de iSCSI 30
 - Sistema: Configuración de NVMe 43
 - Sistema: Funciones complementarias 51
 - Sistema: Gestión de claves de seguridad 55
 - Access Management 71
 - Certificados 104

Configuración

Alertas

Conceptos

¿Cómo funcionan las alertas

Las alertas notifican a los administradores sobre eventos importantes que se producen en la cabina de almacenamiento. Las alertas se pueden enviar por correo electrónico, capturas SNMP y syslog.

El proceso de las alertas funciona de la siguiente manera:

1. Un administrador configura uno o varios de los siguientes métodos de alerta en System Manager:
 - **Correo electrónico** — los mensajes se envían a direcciones de correo electrónico.
 - **SNMP** — las capturas SNMP se envían a un servidor SNMP.
 - **Syslog** — los mensajes se envían a un servidor syslog.
2. Cuando el monitor de eventos de la cabina de almacenamiento detecta un problema, escribe información sobre ese problema en el registro de eventos (disponible en **menú:Soporte[Registro de eventos]**). Por ejemplo, los problemas pueden incluir eventos como un fallo de la batería, un componente que pasa del estado óptimo a sin conexión, o bien errores de redundancia en la controladora.
3. Si el monitor de eventos determina que el evento genera alertas, envía una notificación con los métodos de alerta configurados (correo electrónico, SNMP o syslog). Se considera que todos los eventos críticos generan alertas, junto con algunos eventos informativos y de advertencia.

Configuración de alertas

Es posible configurar alertas en el asistente de configuración inicial (solo para alertas de correo electrónico) o en la página Alertas. Para comprobar la configuración actual, vaya a **MENU:Settings[Alerts]**.

El icono Alertas muestra la configuración de las alertas, que puede ser una de las siguientes:

- No configurado.
- Configurado; se ha configurado al menos un método de alerta. Para determinar qué métodos de alertas están configurados, apunte el cursor al icono.

Información sobre alertas

Las alertas pueden incluir los siguientes tipos de información:

- Nombre de la cabina de almacenamiento.
- Tipo de error de evento relacionado con una entrada del registro de eventos.
- La fecha y la hora en que ocurrió el evento.
- Una breve descripción del evento.



Las alertas de syslog siguen el estándar de mensajería de RFC 3164.

Terminología de alertas

Conozca la forma en que los términos de alertas se aplican a su cabina de almacenamiento.

Componente	Descripción
Monitor de eventos	El monitor de eventos reside en la cabina de almacenamiento y se ejecuta como una tarea en segundo plano. Cuando el monitor de eventos detecta anomalías en la cabina de almacenamiento, escribe información acerca de los problemas en el registro de eventos. Los problemas pueden incluir eventos como un fallo de batería, un componente que pasa de estado óptimo a sin conexión o errores de redundancia en la controladora. Si el monitor de eventos determina que el evento genera alertas, envía una notificación con los métodos de alerta configurados (correo electrónico, SNMP o syslog). Se considera que todos los eventos críticos generan alertas, junto con algunos eventos informativos y de advertencia.
Servidor de correo	El servidor de correo se usa para enviar y recibir alertas de correo electrónico. El servidor utiliza un protocolo para la transferencia simple de correo electrónico (SMTP).
SNMP	El protocolo simple de gestión de redes (SNMP) es un protocolo estándar de Internet que se usa para gestionar y compartir información entre dispositivos en redes de IP.
Captura SNMP	Una captura SNMP es una notificación que se envía a un servidor SNMP. La captura tiene información acerca de problemas importantes en la cabina de almacenamiento.
Destino de capturas SNMP	El destino de una captura SNMP es la dirección IPv4 o IPv6 del servidor que ejecuta un servicio SNMP.
Nombre de comunidad	Un nombre de comunidad es una cadena que actúa como contraseña para el servidor de red en un entorno SNMP.
Archivo MIB	El archivo de base de datos de información de gestión (MIB) define los datos que se están supervisando y gestionando en la cabina de almacenamiento. Se debe copiar y compilar en el servidor mediante la aplicación de servicio SNMP. El archivo MIB está disponible en el software System Manager del sitio de soporte.
Variables MIB	Las variables de la base de datos de información de gestión (MIB) pueden mostrar valores, como el nombre de cabina de almacenamiento, la ubicación de la cabina y una persona de contacto, en respuesta a las solicitudes SNMP GetRequests.
Syslog	Syslog es un protocolo que utilizan los dispositivos de red para enviar mensajes de eventos a un servidor de registro.

Componente	Descripción
UDP	El protocolo de datagramas de usuario (UDP) es un protocolo de capa de transporte que especifica un número de puerto de origen y de destino en los encabezados de paquete.

Procedimientos

Gestionar alertas por correo electrónico

Configurar servidores de correo y destinatarios para las alertas

Para configurar las alertas por correo electrónico, debe indicar una dirección de correo electrónico del servidor y las direcciones de correo electrónico de los destinatarios de las alertas. Está permitido introducir hasta 20 direcciones de correo electrónico.

Antes de empezar

- La dirección del servidor de correo debe estar disponible. La dirección puede ser IPv4 o IPv6, o bien un nombre de dominio completo.



Para usar un nombre de dominio completo, debe configurar un servidor DNS en ambas controladoras. Es posible configurar un servidor DNS desde la página hardware.

- La dirección de correo electrónico que se usará como remitente de alertas debe estar disponible. Esta es la dirección que aparece en el campo "From" del mensaje de alerta. Es necesario contar con una dirección de remitente en el protocolo SMTP; sin esa dirección, se produce un error.
- Las direcciones de correo electrónico de los destinatarios de alertas deben estar disponibles. Por lo general, el destinatario tiene la dirección de un administrador de red o de almacenamiento. Es posible introducir hasta 20 direcciones de correo electrónico.

Acerca de esta tarea

En esta tarea, se describe cómo configurar el servidor de correo, introducir las direcciones de correo electrónico del remitente y de los destinatarios, y analizar todas las direcciones de correo electrónico introducidas desde la página Alertas.



Las alertas por correo electrónico también pueden configurarse en el asistente de configuración inicial.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **correo electrónico**.

Si aún no se configuró ningún servidor de correo, la pestaña correo electrónico muestra "Configure Mail Server".

3. Seleccione **Configurar el servidor de correo**.

Se abre el cuadro de diálogo **Configurar el servidor de correo**.

4. Introduzca la información del servidor de correo y, a continuación, haga clic en **Guardar**.

- **Dirección del servidor de correo** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6 del servidor de correo.



Para usar un nombre de dominio completo, debe configurar un servidor DNS en ambas controladoras. Puede configurar un servidor DNS desde la página **hardware**.

- **Dirección del remitente de correo electrónico** — Introduzca una dirección de correo electrónico válida que se utilizará como remitente del correo electrónico. Esta dirección aparece en el campo "de" del mensaje de correo electrónico.
- **Incluir información de contacto en el correo electrónico** — para incluir la información de contacto del remitente con el mensaje de alerta, seleccione esta opción e introduzca un nombre y un número de teléfono. Después de hacer clic en **Guardar**, las direcciones de correo electrónico aparecerán en la ficha **correo electrónico** de la página **Alertas**.

5. Seleccione **Añadir correos electrónicos**.

Se abre el cuadro de diálogo Añadir correos electrónicos.

6. Introduzca una o más direcciones de correo electrónico para los destinatarios de alertas y, a continuación, haga clic en **Agregar**.

Las direcciones de correo electrónico aparecerán en la página Alertas.

7. Si desea asegurarse de que las direcciones de correo electrónico son válidas, haga clic en **probar todos los correos electrónicos** para enviar mensajes de prueba a los destinatarios.

Resultados

Después de configurar las alertas por correo electrónico, el monitor de eventos envía mensajes de correo electrónico a los destinatarios especificados cada vez que se produce un evento que genera alertas.

Editar direcciones de correo electrónico para alertas

Es posible cambiar las direcciones de correo electrónico de los destinatarios que recibieron alertas por correo electrónico.

Antes de empezar

Las direcciones de correo electrónico que pretende editar deben estar definidas en la pestaña correo electrónico de la página Alertas.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **correo electrónico**.
3. En la tabla **Dirección de correo electrónico**, seleccione la dirección que desea cambiar y, a continuación, haga clic en el icono **Edición** (lápiz) situado en el extremo derecho.

La fila se convierte en un campo editable.

4. Introduzca una dirección nueva y, a continuación, haga clic en el icono **Guardar** (Marca de verificación).



Si desea cancelar los cambios, seleccione el icono **Cancelar** (X).

Resultados

La pestaña correo electrónico de la página Alertas muestra las direcciones de correo electrónico actualizadas.

Añadir direcciones de correo electrónico para alertas

Es posible añadir hasta 20 destinatarios para alertas por correo electrónico.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **correo electrónico**.
3. Seleccione **Añadir correos electrónicos**.

Se abre el cuadro de diálogo **Agregar correos electrónicos**.

4. En el campo vacío, introduzca una nueva dirección de correo electrónico. Si desea agregar más de una dirección, seleccione **Agregar otro correo electrónico** para abrir otro campo.
5. Haga clic en **Agregar**.

Resultados

La ficha **correo electrónico** de la página **Alertas** muestra las nuevas direcciones de correo electrónico.

Eliminar servidor de correo o direcciones de correo electrónico para las alertas

Es posible eliminar el servidor de correo definido previamente para que no se envíen alertas a las direcciones de correo electrónico, o eliminar direcciones de correo electrónico individuales.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **correo electrónico**.
3. Desde la tabla, realice una de las siguientes acciones:
 - Para eliminar un servidor de correo de modo que no se envíen alertas a las direcciones de correo electrónico, seleccione la fila del servidor de correo.
 - Para eliminar una dirección de correo electrónico y no enviar alertas a esta dirección, seleccione la fila de la dirección de correo electrónico que desea eliminar. El botón **Eliminar** de la parte superior derecha de la tabla está disponible para su selección.
4. Haga clic en **Eliminar** y confirme la operación.

Editar servidor de correo para alertas

Es posible cambiar la dirección del servidor de correo y la dirección del remitente de correo utilizada para las alertas por correo electrónico.

Antes de empezar

La dirección del servidor de correo que desea cambiar debe estar disponible. La dirección puede ser IPv4 o IPv6, o bien un nombre de dominio completo.



Para usar un nombre de dominio completo, debe configurar un servidor DNS en ambas controladoras. Es posible configurar un servidor DNS desde la página hardware.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **correo electrónico**.
3. Seleccione **Configurar el servidor de correo**.

Se abre el cuadro de diálogo Configurar el servidor de correo.

4. Edite la dirección del servidor de correo, la información del remitente y la información de contacto.

- **Dirección del servidor de correo** — edite el nombre de dominio completo, la dirección IPv4 o la dirección IPv6 del servidor de correo.



Para usar un nombre de dominio completo, debe configurar un servidor DNS en ambas controladoras. Es posible configurar un servidor DNS desde la página hardware.

- **Dirección del remitente de correo electrónico** — edite la dirección de correo electrónico que se utilizará como remitente del correo electrónico. Esta dirección aparece en el campo "de" del mensaje de correo electrónico.
- **Incluir información de contacto en el correo electrónico** — para editar la información de contacto del remitente, seleccione esta opción y, a continuación, edite el nombre y el número de teléfono.

5. Haga clic en **Guardar**.

Gestionar alertas SNMP

Configurar las comunidades y los destinos para las alertas SNMP

Para configurar alertas del protocolo simple de gestión de redes (SNMP) se debe identificar al menos un servidor en el que el monitor de eventos de la cabina de almacenamiento pueda enviar capturas SNMP. La configuración requiere un nombre de comunidad y una dirección IP para el servidor.

Antes de empezar

- Debe configurarse un servidor de red con una aplicación de servicio SNMP. Es necesario tener la dirección de red de este servidor (ya sea una dirección IPv4 o IPv6), de manera que el monitor de eventos pueda enviar mensajes de captura a esa dirección. Es posible usar más de un servidor (se permiten hasta 10 servidores).
- Debe crearse un nombre de comunidad, que consiste únicamente en caracteres ASCII imprimibles. Un administrador de red suele crear el nombre de comunidad, que es una cadena que actúa como contraseña para los servidores de red. Es posible crear hasta 256 comunidades.
- El archivo de base de datos de información de gestión (MIB) se copió y compiló en el servidor con la aplicación de servicio SNMP. Este archivo MIB define los datos que se están supervisando y gestionando.

Si no tiene el archivo MIB, puede obtenerlo en el sitio de soporte de NetApp:

- Vaya a. "[Soporte de NetApp](#)".
- Haga clic en **Descargas**.
- Haga clic en **Software**.
- Busque el software de gestión (por ejemplo, Administrador del sistema de SANtricity) y, a continuación, haga clic en **Ir** a la derecha.

- Haga clic en **Ver y descargar** en la última versión.
- Haga clic en **continuar** en la parte inferior de la página.
- Acepte el contrato de licencia para usuario final.
- Desplácese hacia abajo hasta que vea **Archivo MIB para capturas SNMP** y haga clic en el enlace para descargar el archivo.

Acerca de esta tarea

En esta tarea, se describe cómo identificar el servidor SNMP para el destino de capturas y, a continuación, poner a prueba la configuración.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **SNMP**.

Si aún no se configuró la comunidad, se muestra "Configure Communities" en la pestaña SNMP.

3. Seleccione **Configurar comunidades**.

Se abre el cuadro de diálogo **Configurar comunidades**.

4. En el campo **Nombre de comunidad**, introduzca una o más cadenas de comunidad para los servidores de red y, a continuación, haga clic en **Guardar**.

En la página Alertas, se muestra "Añadir destinos de captura".

5. Seleccione **Añadir destinos de captura**.

Se abre el cuadro de diálogo **Agregar destinos de captura**.

6. Introduzca uno o más destinos de captura, seleccione los nombres de comunidad asociados y, a continuación, haga clic en **Agregar**.
 - **Destino de captura** — Introduzca una dirección IPv4 o IPv6 del servidor que ejecuta un servicio SNMP.
 - **Nombre de comunidad** — en el menú desplegable, seleccione el nombre de comunidad para este destino de captura. (Si definió solo un nombre de comunidad, ese nombre ya aparece en este campo.)
 - **Enviar captura de fallo de autenticación** — Seleccione esta opción (la casilla de verificación) si desea alertar al destino de la captura cada vez que se rechace una solicitud SNMP debido a un nombre de comunidad no reconocido. Después de hacer clic en **Agregar**, los destinos de captura y los nombres de comunidad asociados aparecen en la ficha **SNMP** de la página **Alertas**.
7. Para asegurarse de que una captura es válida, seleccione un destino de captura de la tabla y, a continuación, haga clic en **probar destino de captura** para enviar una captura de prueba a la dirección configurada.

Resultados

El monitor de eventos envía capturas SNMP a los servidores cada vez que ocurre un evento que genera alertas.

Editar nombres de comunidad para capturas SNMP

Puede editar nombres de comunidades para capturas SNMP y también asociar un

nombre de comunidad diferente para un destino de captura SNMP.

Antes de empezar

Debe crearse un nombre de comunidad, que consiste únicamente en caracteres ASCII imprimibles. Un administrador de red crea el nombre de comunidad, que es una cadena que actúa como contraseña para los servidores de red.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **SNMP**.

Los destinos de capturas y los nombres de comunidad aparecen en la tabla.

3. Edite los nombres de comunidad de la siguiente manera:
 - Para editar un nombre de comunidad, seleccione **Configurar comunidades**. Introduzca el nuevo nombre de comunidad y haga clic en **Guardar**. Los nombres de comunidades deben consistir únicamente en caracteres ASCII imprimibles.
 - Para asociar un nombre de comunidad a un nuevo destino de captura, seleccione el nombre de comunidad de la tabla y, a continuación, haga clic en el icono **Editar** (lápiz) situado en el extremo derecho. En la lista desplegable Nombre de comunidad, seleccione un nombre de comunidad nuevo para un destino de captura SNMP y, a continuación, haga clic en el icono **Guardar** (Marca de verificación).



Si desea cancelar los cambios, seleccione el icono **Cancelar** (X).

Resultados

La ficha **SNMP** de la página **Alertas** muestra las comunidades actualizadas.

Añadir nombres de comunidad para capturas SNMP

Se pueden añadir hasta 256 nombres de comunidad para las capturas SNMP.

Antes de empezar

Se deben crear los nombres de comunidad. Un administrador de red suele crear el nombre de comunidad, que es una cadena que actúa como contraseña para los servidores de red. Está compuesto solo por caracteres ASCII que se pueden imprimir.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **SNMP**.

Los destinos de capturas y los nombres de comunidad aparecen en la tabla.

3. Seleccione **Configurar comunidades**.

Se abre el cuadro de diálogo Configurar comunidades.

4. Seleccione **Añadir otra comunidad**.
5. Introduzca el nuevo nombre de comunidad y haga clic en **Guardar**.

Resultados

El nuevo nombre de comunidad aparece en la pestaña **SNMP** de la página **Alertas**.

Quitar un nombre de comunidad de las capturas de SNMP

Es posible quitar un nombre de comunidad de las capturas de SNMP.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **SNMP**.

Los nombres de comunidad y los destinos de captura se muestran en la página **Alertas**.

3. Seleccione **Configurar comunidades**.

Se abre el cuadro de diálogo **Configurar comunidades**.

4. Seleccione el nombre de comunidad que desea eliminar y, a continuación, haga clic en el icono **Quitar (X)** situado en el extremo derecho.

Si los destinos de captura están asociados con este nombre de comunidad, el cuadro de diálogo **Confirmar eliminación de comunidad** muestra las direcciones de destino de captura afectadas.

5. Confirme la operación y haga clic en **Quitar**.

Resultados

El nombre de comunidad y su destino de captura asociado se eliminan de la página **Alertas**.

Configure las variables MIB de SNMP

En el caso de las alertas SNMP, tiene la opción de configurar las variables de la base de datos de información de gestión (MIB) que se muestran en las excepciones SNMP. Estas variables pueden mostrar el nombre de la cabina de almacenamiento, su ubicación y una persona de contacto.

Antes de empezar

El archivo MIB debe copiarse y compilarse en el servidor con la aplicación de servicio SNMP.

Si no tiene un archivo MIB, puede obtenerlo del siguiente modo:

- Vaya a ["Soporte de NetApp"](#).
- Haga clic en **Descargas**.
- Haga clic en **Software**.
- Busque el software de gestión (por ejemplo, Administrador del sistema de SANtricity) y, a continuación, haga clic en **Ir** a la derecha.
- Haga clic en **Ver y descargar** en la última versión.
- Haga clic en **continuar** en la parte inferior de la página.
- Acepte el contrato de licencia para usuario final.
- Desplácese hacia abajo hasta que vea **Archivo MIB para capturas SNMP** y haga clic en el enlace para descargar el archivo.

Acerca de esta tarea

En esta tarea, se describe cómo definir variables MIB para excepciones SNMP. Estas variables pueden mostrar los siguientes valores, en respuesta a los mensajes GetRequests de SNMP:

- *sysName* (nombre para la cabina de almacenamiento)
- *sysLocation* (ubicación de la cabina de almacenamiento)
- *sysContact* (nombre de un administrador)

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **SNMP**.
3. Seleccione **Configurar variables MIB de SNMP**.

Se muestra el cuadro de diálogo Configurar variables MIB de SNMP.

4. Introduzca uno o más de los siguientes valores y, a continuación, haga clic en **Guardar**.
 - **Nombre** — el valor de la variable MIB *sysName*. Por ejemplo, introduzca un nombre para la cabina de almacenamiento.
 - **Ubicación** — el valor de la variable MIB *sysLocation*. Por ejemplo, introduzca la ubicación de la cabina de almacenamiento.
 - **Contacto** — el valor de la variable MIB *sysContact*. Por ejemplo, introduzca un administrador que sea responsable de la cabina de almacenamiento.

Resultados

Estos valores se muestran en los mensajes de captura SNMP en las alertas de la cabina de almacenamiento.

Añadir destinos de capturas para alertas SNMP

Es posible añadir hasta 10 servidores para enviar capturas SNMP.

Antes de empezar

- El servidor de red que desea añadir debe estar configurado con una aplicación de servicio SNMP. Es necesario tener la dirección de red de este servidor (ya sea una dirección IPv4 o IPv6), de manera que el monitor de eventos pueda enviar mensajes de captura a esa dirección. Es posible usar más de un servidor (se permiten hasta 10 servidores).
- Debe crearse un nombre de comunidad, que consiste únicamente en caracteres ASCII imprimibles. Un administrador de red suele crear el nombre de comunidad, que es una cadena que actúa como contraseña para los servidores de red. Es posible crear hasta 256 comunidades.
- El archivo de base de datos de información de gestión (MIB) se copió y compiló en el servidor con la aplicación de servicio SNMP. Este archivo MIB define los datos que se están supervisando y gestionando.

Si no tiene el archivo MIB, puede obtenerlo en el sitio de soporte de NetApp:

- Vaya a. ["Soporte de NetApp"](#).
- Haga clic en **Descargas**.
- Haga clic en **Software**.
- Busque el software de gestión (por ejemplo, Administrador del sistema de SANtricity) y, a continuación,

haga clic en **Ir** a la derecha.

- Haga clic en **Ver y descargar** en la última versión.
- Haga clic en **continuar** en la parte inferior de la página.
- Acepte el contrato de licencia para usuario final.
- Desplácese hacia abajo hasta que vea **Archivo MIB para capturas SNMP** y haga clic en el enlace para descargar el archivo.

Pasos

1. Seleccione **Ajustes > Alertas**.
2. Seleccione la ficha **SNMP**.

Los destinos de capturas definidos actualmente se muestran en la tabla.

3. Seleccione **Agregar destinos de captura**.

Se abre el cuadro de diálogo Añadir destinos de captura.

4. Introduzca uno o más destinos de captura, seleccione los nombres de comunidad asociados y, a continuación, haga clic en **Agregar**.
 - **Destino de captura** — Introduzca una dirección IPv4 o IPv6 del servidor que ejecuta un servicio SNMP.
 - **Nombre de comunidad** — en el menú desplegable, seleccione el nombre de comunidad para este destino de captura. (Si definió solo un nombre de comunidad, ese nombre ya aparece en este campo.)
 - **Enviar captura de fallo de autenticación** — Seleccione esta opción (la casilla de verificación) si desea alertar al destino de la captura cada vez que se rechace una solicitud SNMP debido a un nombre de comunidad no reconocido. Después de hacer clic en **Agregar**, los destinos de captura y los nombres de comunidad asociados aparecen en la tabla.
5. Para asegurarse de que una captura es válida, seleccione un destino de captura de la tabla y, a continuación, haga clic en **probar destino de captura** para enviar una captura de prueba a la dirección configurada.

Resultados

El monitor de eventos envía capturas SNMP a los servidores cada vez que ocurre un evento que genera alertas.

Eliminar destinos de capturas

Es posible eliminar una dirección de destino de captura para que el monitor de eventos de la cabina de almacenamiento ya no envíe capturas SNMP a esa dirección.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **SNMP**.

Las direcciones de los destinos de captura se muestran en la tabla.

3. Seleccione un destino de captura y, a continuación, haga clic en **Eliminar** en la esquina superior derecha de la página.
4. Confirme la operación y haga clic en **Eliminar**.

La dirección de destino ya no aparece en la página **Alertas**.

Resultados

El destino de captura eliminado ya no recibe capturas SNMP del monitor de eventos de la cabina de almacenamiento.

Gestionar alertas de syslog

Configurar el servidor de syslog para las alertas

Para configurar alertas de syslog, debe introducir una dirección de servidor de syslog y un puerto UDP. Se permiten hasta cinco servidores de syslog.

Antes de empezar

- Debe estar disponible la dirección del servidor de syslog. La dirección debe ser un nombre de dominio completo o una dirección IPv4 o IPv6.
- El número de puerto UDP del servidor de syslog debe estar disponible. Por lo general, se trata del puerto 514.

Acerca de esta tarea

En esta tarea, se describe cómo introducir la dirección y el puerto de un servidor de syslog, y después probar la dirección introducida.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **Syslog**.

Si aún no se ha definido un servidor de syslog, la página **Alertas** muestra "Agregar servidores de syslog".

3. Haga clic en **Agregar servidores de syslog**.

Se abrirá el cuadro de diálogo **Agregar servidor de syslog**.

4. Introduzca información para uno o más servidores de syslog (hasta un máximo de cinco) y, a continuación, haga clic en **Agregar**.
 - **Dirección del servidor** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
 - **Puerto UDP** — por lo general, el puerto UDP para syslog es 514. En la tabla, se presentan los servidores de syslog configurados.
5. Para enviar una alerta de prueba a las direcciones del servidor, seleccione **probar todos los servidores de syslog**.

Resultados

El monitor de eventos envía alertas al servidor de syslog cada vez que ocurre un evento que genera alertas.

Edite los servidores de syslog para las alertas

Es posible editar la dirección de servidor utilizada para recibir alertas de syslog.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **Syslog**.
3. En la tabla, seleccione una dirección de servidor de syslog y, a continuación, haga clic en el icono **Editar** (lápiz) situado en el extremo derecho.

La fila se convierte en un campo editable.

4. Edite la dirección de servidor y el número de puerto UDP y, a continuación, haga clic en el icono **Guardar** (Marca de verificación).

Resultados

La dirección actualizada del servidor se muestra en la tabla.

Añada servidores de syslog para alertas

Es posible añadir un máximo de cinco servidores para las alertas de syslog.

Antes de empezar

- Debe estar disponible la dirección del servidor de syslog. La dirección debe ser un nombre de dominio completo o una dirección IPv4 o IPv6.
- Debe estar disponible el número de puerto UDP del servidor de syslog. Por lo general, se trata del puerto 514.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **Syslog**.
3. Seleccione **Agregar servidores de syslog**.

Se abre el cuadro de diálogo Añadir servidor de syslog.

4. Seleccione **Añadir otro servidor de syslog**.
5. Introduzca información para el servidor syslog y, a continuación, haga clic en **Agregar**.

- **Dirección del servidor Syslog** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- **Puerto UDP** — por lo general, el puerto UDP para syslog es 514.



Es posible configurar hasta cinco servidores de syslog.

Resultados

Las direcciones del servidor de syslog aparecen en la tabla.

Elimine los servidores de syslog para las alertas

Es posible eliminar un servidor de syslog para que no siga recibiendo alertas.

Pasos

1. Seleccione **MENU:Settings[Alerts]**.
2. Seleccione la ficha **Syslog**.

3. Seleccione una dirección de servidor de syslog y haga clic en **Quitar** en la parte superior derecha.

Se abrirá el cuadro de diálogo Confirmar eliminación de servidor de syslog.

4. Confirme la operación y haga clic en **Eliminar**.

Resultados

El servidor que ha eliminado ya no recibe alertas del monitor de eventos.

Preguntas frecuentes

¿Qué sucede si se deshabilitan las alertas?

Si desea que los administradores reciban notificaciones sobre eventos importantes que suceden en la cabina de almacenamiento, se debe configurar un método de alerta.

Para las cabinas de almacenamiento gestionadas con SANtricity System Manager, es posible configurar alertas desde la página Alertas. Las notificaciones de alerta se pueden enviar por correo electrónico, capturas SNMP o mensajes de syslog. Además, las alertas por correo electrónico pueden configurarse desde el asistente de configuración inicial.

¿Cómo se configuran las alertas de SNMP o syslog?

Además de las alertas por correo electrónico, es posible configurar el envío de alertas mediante capturas de protocolo simple de gestión de redes (SNMP) o mensajes de syslog.

Para configurar las alertas de SNMP o syslog, vaya a MENU:Configuración[Alertas].

¿Por qué las marcas de tiempo no son consistentes entre la cabina y las alertas?

Cuando la cabina de almacenamiento envía alertas, no corrige la zona horaria según el host o servidor de destino que recibe las alertas. En cambio, la cabina de almacenamiento utiliza la hora local (GMT) para crear la Marca de tiempo que se utiliza para el registro de alertas. Como resultado, es posible que se observen inconsistencias entre las marcas de tiempo de la cabina de almacenamiento y el servidor o host que recibe una alerta.

Debido a que la cabina de almacenamiento no corrige la zona horaria cuando envía alertas, la Marca de tiempo de las alertas está en horario GMT, que tiene un valor cero de desfase de zona horaria. Para calcular una Marca de tiempo adecuada para su zona horaria local, debe determinar el desfase de su zona horaria respecto a GMT y sumar o restar ese valor a las marcas de tiempo.



Para evitar esto, configure el protocolo de tiempo de redes (NTP) en las controladoras de la cabina de almacenamiento. NTP se asegura de que las controladoras siempre estén sincronizadas con la hora correcta.

Sistema: Configuración de la cabina de almacenamiento

Conceptos

Rendimiento y configuración de la caché

La memoria caché es un área de almacenamiento volátil temporal en la controladora que tiene un tiempo de acceso menor que los medios con unidades.

Con el almacenamiento en caché, es posible aumentar el rendimiento de I/O de la siguiente manera:

- Los datos solicitados desde el host para una lectura pueden estar ya en la caché debido a una operación anterior. Esto elimina la necesidad de acceder a la unidad.
- Los datos de escritura se escriben primero en la caché. Esto permite que la aplicación avance sin esperar que los datos se escriban en la unidad.

La configuración predeterminada de la caché cumple con los requisitos de la mayoría de los entornos, pero es posible modificarla si es necesario.

Configuración de la caché de la cabina de almacenamiento

Es posible especificar los siguientes valores en la página sistema para todos los volúmenes de la cabina de almacenamiento:

- **Iniciar valor para vaciar** — el porcentaje de datos no escritos en la caché que activan un vaciado de caché (escribir en disco). Cuando la caché alberga el porcentaje de inicio especificado de datos sin escribir, se activa un vaciado. De forma predeterminada, la controladora inicia el vaciado de la caché cuando la caché se encuentra un 80 % llena.
- **Tamaño de bloque de caché** — el tamaño máximo de cada bloque de caché, que es una unidad organizativa para la administración de caché. De forma predeterminada, el tamaño de bloque de caché es 8 KiB, pero se puede establecer en 4, 8, 16 o 32 KiB. Lo ideal es establecer el tamaño de bloque de caché en el tamaño de I/O predominante de las aplicaciones. Por lo general, los sistemas de archivos o las aplicaciones de bases de datos utilizan tamaños menores. Se recomiendan tamaños mayores para las aplicaciones de grandes transferencias de datos o I/O secuenciales

Configuración de la caché del volumen

Es posible especificar los siguientes valores en la página volúmenes para volúmenes individuales de la cabina de almacenamiento (menú:almacenamiento[volumenes]):

- **Caché de lectura** — la caché de lectura es un búfer que almacena datos que se han leído desde las unidades. Es posible que los datos de una operación de lectura ya deban estar en la caché debido a una operación anterior, por lo tanto, no es necesario acceder a las unidades. Los datos se conservan en la caché de lectura hasta que esta se vacía.
 - **Captura previa de caché de lectura dinámica:** La captura previa de lectura de caché dinámica permite a la controladora copiar otros bloques de datos secuenciales en la caché mientras lee bloques de datos de una unidad en la caché. Ese almacenamiento en caché aumenta la posibilidad de que se puedan cumplir futuras solicitudes de datos de la caché. La captura previa de lectura de la caché dinámica es importante para las aplicaciones multimedia que utilizan I/O secuencial. La cantidad y la velocidad de las capturas previas de los datos en la caché se ajustan automáticamente según la velocidad y el tamaño de solicitud de las lecturas del host. El acceso aleatorio no provoca la captura previa de los datos en la caché. Esta función no se aplica cuando el almacenamiento en caché de lectura está deshabilitado.
- **Almacenamiento en caché de escritura** — la caché de escritura es un búfer que almacena datos del host que todavía no se han escrito en las unidades. Los datos permanecen en la caché de escritura hasta

que se escriben en las unidades. El almacenamiento en caché de escritura puede aumentar el rendimiento de I/O.



Posible pérdida de datos — Si activa la opción almacenamiento en caché de escritura sin baterías y no dispone de una fuente de alimentación universal de protección, podría perder datos. Además, es posible perder datos si la controladora no tiene baterías y se habilita la opción almacenamiento en caché de escritura sin baterías.

- **Almacenamiento en caché de escritura sin baterías** — la configuración de almacenamiento en caché de escritura sin baterías permite que el almacenamiento en caché de escritura continúe incluso cuando las baterías faltan, fallan, están completamente descargadas o no están totalmente cargadas. Por lo general, no se recomienda elegir el almacenamiento en caché de escritura sin baterías porque se pueden perder los datos en caso de interrupción del suministro eléctrico. Comúnmente, la controladora desactiva en forma temporal el almacenamiento en caché de escritura hasta que se cargan las baterías o se reemplaza una batería con errores.
- **Almacenamiento en caché de escritura con duplicación** — el almacenamiento en caché de escritura con duplicación se produce cuando los datos escritos en la memoria caché de un controlador también se escriben en la memoria caché del otro controlador. Por lo tanto, si una controladora falla, la otra puede completar todas las operaciones de escritura pendientes. El mirroring de la caché de escritura está disponible solo si el almacenamiento en caché de escritura está habilitado y existen dos controladoras. El almacenamiento en caché de escritura con mirroring es la configuración predeterminada cuando se crea un volumen.

Información general sobre equilibrio de carga automático

La función Automatic Load Balancing ofrece una gestión de recursos de I/O mejorada, ya que reacciona dinámicamente a los cambios de carga con el tiempo y ajusta automáticamente la propiedad de la controladora de volumen para corregir cualquier problema de desequilibrio de carga cuando las cargas de trabajo son distintas de una controladora a otra.

La carga de trabajo de cada controladora se supervisa continuamente y, con la colaboración de los controladores multivía instalados en los hosts, es posible establecer automáticamente el equilibrio cada vez que sea necesario. Una vez que la carga de trabajo se vuelve a equilibrar de forma automática en todas las controladoras, el administrador de almacenamiento queda liberado de la carga que supone ajustar manualmente la propiedad de la controladora de volumen para admitir cambios de carga en la cabina de almacenamiento.

Cuando la función Automatic Load Balancing está habilitada, ejecuta las siguientes funciones:

- Supervisa y equilibra automáticamente la utilización de recursos de la controladora.
- Ajusta automáticamente la propiedad de la controladora de volumen cuando es necesario y así, optimiza el ancho de banda de I/O entre los hosts y la cabina de almacenamiento.

Habilitar y deshabilitar Automatic Load Balancing

La función Automatic Load Balancing está habilitada de forma predeterminada en todas las cabinas de almacenamiento.

Puede ser conveniente deshabilitar Automatic Load Balancing en la cabina de almacenamiento por las siguientes razones:

- No se desea cambiar automáticamente la propiedad de una controladora de volumen para equilibrar la carga de trabajo.
- Se trabaja en un entorno altamente optimizado donde la distribución de carga se configura intencionalmente para lograr una distribución específica entre las controladoras.

Los tipos de hosts compatibles con la función Automatic Load Balancing

Aunque la función Automatic Load Balancing está habilitada en el nivel de la cabina de almacenamiento, el tipo de host que se selecciona para un host o clúster de hosts tiene una influencia directa sobre la forma en que opera la función.

Cuando se equilibra la carga de trabajo de la cabina de almacenamiento en varias controladoras, la función Automatic Load Balancing intenta mover volúmenes a los que pueden acceder ambas controladoras y que solo se asignan a un host o clúster de hosts compatible con la función Automatic Load Balancing.

Este comportamiento evita que un host pierda acceso a un volumen debido al proceso de equilibrio de carga; sin embargo, la presencia de volúmenes asignados a hosts no compatibles con Automatic Load Balancing afecta a la capacidad para equilibrar la carga de trabajo que posee la cabina de almacenamiento. Para que Automatic Load Balancing equilibre la carga de trabajo, el controlador multivía debe ser compatible con TPGS, y debe incluirse el tipo de host en la siguiente tabla.



Para que un clúster de hosts se considere compatible con Automatic Load Balancing, todos los hosts de ese grupo deben ser compatibles con Automatic Load Balancing.

Tipo de host compatible con Automatic Load Balancing	Con este controlador multivía
Windows o Windows almacenado en clúster	MPIO con DSM E-Series de NetApp
Linux DM-MP (Kernel 3.10 o posterior)	DM-MP con <code>scsi_dh_alua</code> controlador de dispositivos
VMware	Complemento nativo multivía (NMP) con <code>VMW_SATP_ALUA</code> Storage Array Type plugin



Salvo excepciones menores, los tipos de hosts no compatibles con Automatic Load Balancing siguen funcionando normalmente más allá de que la función esté habilitada o no. Una excepción es cuando un sistema conmuta al nodo de respaldo y las cabinas de almacenamiento mueven volúmenes sin asignar nuevamente a la controladora a la que pertenecen cuando la ruta de datos regresa. No se mueve ninguno de los volúmenes asignados a hosts no compatibles con Automatic Load Balancing.

Consulte "[Herramienta de matriz de interoperabilidad](#)" Para acceder a información de compatibilidad para controladores multivía específicos, nivel de sistema operativo y compatibilidad con soportes de controladoras-unidades.

Comprobación de la compatibilidad del sistema operativo con la función Automatic Load Balancing

Compruebe la compatibilidad del sistema operativo con la función Automatic Load Balancing antes de configurar un sistema nuevo o migrar uno existente.

1. Vaya a la "[Herramienta de matriz de interoperabilidad](#)" para encontrar la solución y verificar la compatibilidad.

Si el sistema operativo es Red Hat Enterprise Linux 6 o SUSE Linux Enterprise Server 11, póngase en contacto con el servicio de asistencia técnica.

2. Actualice y configure el `/etc/multipath.conf` file.
3. Asegúrese de que ambos `retain_attached_device_handler` y `detect_prio` se establecen en `yes` para el proveedor y el producto correspondientes, o utilice la configuración predeterminada.

Tipo de sistema operativo del host predeterminado

La cabina de almacenamiento utiliza el tipo de host predeterminado cuando se conectan inicialmente los hosts. Define la manera en que funcionan las controladoras en la cabina de almacenamiento con el sistema operativo del host cuando se accede a los volúmenes. Es posible cambiar el tipo de host si hay una necesidad de cambiar la manera en que opera la cabina de almacenamiento en relación con los hosts que están conectados con ella.

En general, se debe cambiar el tipo de host predeterminado antes de conectar hosts a la cabina de almacenamiento o al añadir hosts adicionales.

Tenga en cuenta estas directrices:

- Si todos los hosts que piensa conectar a la cabina de almacenamiento tienen el mismo sistema operativo (entorno de host homogéneo), cambie el tipo de host para que coincida con el sistema operativo.
- Si hay hosts con diferentes sistemas operativos que piensa conectar a la cabina de almacenamiento (entorno de host heterogéneo), cambie el tipo de host para que coincida con la mayoría de los sistemas operativos de los hosts.

Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y seis de ellos tienen un sistema operativo Windows, debe seleccionar Windows como tipo de sistema operativo de host predeterminado.

- Si la mayoría de los hosts conectados poseen una combinación de sistemas operativos diferentes, cambie el tipo de host a opción predeterminada de fábrica.

Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y dos de ellos tienen un sistema operativo Windows, tres ejecutan un sistema operativo VMware, Y otros tres ejecutan un sistema operativo Linux, debe seleccionar opción predeterminada de fábrica como el tipo de sistema operativo del host predeterminado.

Procedimientos

Edite el nombre de la cabina de almacenamiento

Es posible cambiar el nombre de la cabina de almacenamiento que aparece en la barra de título de SANtricity System Manager.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **General**, busque el campo **Nombre**:

Si no se definió un nombre de cabina de almacenamiento, este campo muestra el texto "Unknown".

3. Haga clic en el icono **Editar** (lápiz) ubicado junto al nombre de la cabina de almacenamiento.

Ahora el campo puede editarse.

4. Introduzca un nombre nuevo.

Un nombre puede contener letras, números y los caracteres especiales subrayado (_), guión (-) y signo numeral (#). Un nombre no puede contener espacios. Un nombre puede contener un máximo de 30 caracteres. El nombre debe ser único.

5. Haga clic en el icono **Guardar** (Marca de verificación).



Si desea cerrar el campo editable sin realizar cambios, haga clic en el icono **Cancelar** (X).

Resultados

El nuevo nombre aparecerá en la barra de título de SANtricity System Manager.

Encender luces de localización en cabina de almacenamiento

Para encontrar la ubicación física de una cabina de almacenamiento en un armario, se pueden encender las luces (LED) localizadoras.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **General**, haga clic en **encender las luces localizadoras de la matriz de almacenamiento**.

Se abre el cuadro de diálogo **encender las luces localizadoras de la matriz de almacenamiento** y se encienden las luces localizadoras de la matriz de almacenamiento correspondiente.

3. Cuando haya localizado físicamente la cabina de almacenamiento, regrese al cuadro de diálogo y seleccione **Apagar**.

Resultados

Las luces localizadoras se apagan y el cuadro de diálogo se cierra.

Sincronice los relojes de la cabina de almacenamiento

Si el protocolo de tiempo de redes (NTP) no está habilitado, los relojes de las controladoras se pueden configurar manualmente, de manera que queden sincronizados con el cliente de gestión (el sistema que se utiliza para ejecutar el explorador que accede a System Manager de SANtricity).

Acerca de esta tarea

La sincronización garantiza que las marcas de tiempo del evento del registro de eventos coincidan con las marcas de tiempo escritas en los archivos de registro del host. Durante el proceso de sincronización, las controladoras siguen estando disponibles y siguen siendo operativas.



Si la opción NTP se encuentra habilitada en System Manager, no se debe usar esta opción para sincronizar los relojes. En cambio, NTP sincroniza automáticamente los relojes con un host externo que utiliza el protocolo de tiempo de redes simple (SNTP).



Una vez que se realiza la sincronización, se puede observar que las estadísticas de rendimiento se pierden o se alteran, las programaciones se ven afectadas (ASUP, snapshots, etc.) y las marcas de tiempo de los datos de registro se alteran. Para evitar este problema, se puede usar NTP.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **General**, haga clic en **Sincronizar relojes de cabinas de almacenamiento**.

Se abre el cuadro de diálogo Sincronizar relojes de cabinas de almacenamiento. Muestra la fecha y hora actuales de la controladora y el equipo que se usa como cliente de gestión.



Para las cabinas de almacenamiento simples, solo se muestra una controladora.

3. Si las horas que aparecen en el cuadro de diálogo no coinciden, haga clic en **Sincronizar**.

Resultados

Una vez que la sincronización se haya realizado correctamente, las marcas de tiempo del evento serán las mismas para el registro de eventos y los registros de host.

Guarde la configuración de la cabina de almacenamiento

Es posible guardar la información de configuración de una cabina de almacenamiento en un archivo de script para ahorrar tiempo al configurar cabinas de almacenamiento adicionales con las mismas opciones.

Antes de empezar

La cabina de almacenamiento no debe estar sujeta a ninguna operación por la que se modifique su configuración lógica. Algunos ejemplos de estas operaciones son crear o eliminar volúmenes, descargar firmware de controladora, asignar o modificar unidades de repuesto, o añadir capacidad (unidades) a un grupo de volúmenes.

Acerca de esta tarea

Al guardar la configuración de una cabina de almacenamiento, se genera un script de interfaz de línea de comandos (CLI) con las opciones de la cabina de almacenamiento, la configuración de los volúmenes, la configuración de los hosts o las asignaciones de host a volumen para la cabina de almacenamiento. Se puede usar este script de CLI generado para replicar una configuración a otra cabina de almacenamiento con la misma configuración de hardware.

No obstante, no se debe usar este script de CLI para la recuperación ante desastres. En lugar de eso, para restaurar el sistema, utilice el archivo de backup de base de datos de configuración que creó manualmente o póngase en contacto con el soporte técnico para obtener estos datos de los datos de AutoSupport más recientes.

Esta operación *not* guarda estos valores:

- Duración de la batería

- Hora del día de la controladora
- Opciones de la memoria estática de acceso aleatorio no volátil (NVSRAM)
- Funciones excepcionales
- Contraseña de la cabina de almacenamiento
- Estado operativo y estados de los componentes de hardware
- Estado operativo (excepto que sea óptimo) y estados de los grupos de volúmenes
- Servicios de copia, como el mirroring y la copia de volumen



Riesgo de errores en la aplicación — no utilice esta opción si la matriz de almacenamiento está sufriendo una operación que cambiará cualquier configuración lógica. Algunos ejemplos de estas operaciones son crear o eliminar volúmenes, descargar firmware de controladora, asignar o modificar unidades de repuesto, o añadir capacidad (unidades) a un grupo de volúmenes.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Seleccione **Guardar configuración de la matriz de almacenamiento**.
3. Seleccione los elementos de la configuración que desea guardar:
 - **Configuración de la matriz de almacenamiento**
 - **Configuración de volumen**
 - **Configuración del host**
 - **Asignaciones de host a volumen**



Si selecciona el elemento **asignaciones de host a volumen**, el elemento **Configuración de volumen** y el elemento **Configuración de host** también se seleccionan de forma predeterminada. No puede guardar **asignaciones de host a volumen** sin guardar también **Configuración de volumen** y **Configuración de host**.

4. Haga clic en **Guardar**.

El archivo se guarda en la carpeta de descargas del explorador con el nombre `storage-array-configuration.cfg`.

Después de terminar

Para cargar la configuración guardada de una cabina de almacenamiento en otra cabina de almacenamiento, utilice la interfaz de línea de comandos de SANtricity (SMcli) con el `-f` para aplicar la `.cfg` archivo.



También puede cargar la configuración de una cabina de almacenamiento en otras cabinas de almacenamiento mediante la interfaz de Unified Manager (seleccione **menú:gestionar[Importar configuración]**).

Borrar la configuración de la cabina de almacenamiento

Use la operación Clear Configuration cuando desee eliminar todos los pools, los grupos de volúmenes, los volúmenes, las definiciones de hosts y las asignaciones de hosts de la cabina de almacenamiento.

Antes de empezar

- Antes de borrar la configuración de la cabina de almacenamiento, realice un backup de los datos.

Acerca de esta tarea

Clear Storage Array Configuration contiene dos opciones:

- **Volumen:** Normalmente, puede utilizar la opción volumen para volver a configurar una matriz de almacenamiento de prueba como una matriz de almacenamiento de producción. Por ejemplo, puede configurar una cabina de almacenamiento para pruebas y después, una vez terminadas las pruebas, eliminar la configuración de prueba y configurar la cabina de almacenamiento para un entorno de producción.
- **Storage Array:** Normalmente, puede utilizar la opción Storage Array para mover una matriz de almacenamiento a otro departamento o grupo. Por ejemplo, puede que utilice una cabina de almacenamiento en Engineering y ahora Engineering consigue una nueva cabina de almacenamiento, por lo que desea mover la cabina de almacenamiento actual a Administración para volver a configurarla.

La opción cabina de almacenamiento elimina algunas opciones de configuración adicionales.

	Volumen	Cabina de almacenamiento
Elimina pools y grupos de volúmenes	X	X
Elimina volúmenes	X	X
Elimina hosts y clústeres de hosts	X	X
Elimina asignaciones de hosts	X	X
Elimina el nombre de la cabina de almacenamiento		X
Restablece la configuración de caché de la cabina de almacenamiento a su valor predeterminado		X



Riesgo de pérdida de datos — esta operación elimina todos los datos de la matriz de almacenamiento. (No ejecuta un borrado seguro.) No es posible cancelar esta operación una vez que se inicia. Realice esta operación solo cuando el soporte técnico se lo indique.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Seleccione **Borrar configuración de la matriz de almacenamiento**.
3. En la lista desplegable, seleccione **volumen** o **matriz de almacenamiento**.
4. **Opcional:** Si desea guardar la configuración (no los datos), utilice los vínculos del cuadro de diálogo.
5. Confirme que desea llevar a cabo la operación.

Resultados

- La configuración actual se elimina y se destruyen todos los datos existentes de la cabina de

almacenamiento.

- Todas las unidades quedan sin asignar.

Configure el banner de inicio de sesión

Puede crear un banner de inicio de sesión que se presente a los usuarios antes de que puedan establecer sesiones en System Manager de SANtricity. El banner puede incluir un aviso de asesoría y un mensaje de consentimiento.

Acerca de esta tarea

Al crear un banner, este aparece antes de la pantalla de inicio de sesión en un cuadro de diálogo.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En la sección **General**, seleccione **Configurar banner de inicio de sesión**.

Se abre el cuadro de diálogo Configurar banner de inicio de sesión.

3. Introduzca el texto que desea que aparezca en el banner de inicio de sesión.



No use formato HTML ni otras etiquetas de marcado.

4. Haga clic en **Guardar**.

Resultados

La próxima vez que los usuarios inicien sesión en System Manager, el texto se abrirá en un cuadro de diálogo. Los usuarios deben hacer clic en **Aceptar** para continuar con la pantalla de inicio de sesión.

Gestionar los tiempos de espera de sesión

Es posible configurar los tiempos de espera en SANtricity System Manager para que las sesiones inactivas de los usuarios se desconecten después de un periodo especificado.

Acerca de esta tarea

De manera predeterminada, el tiempo de espera de sesión para System Manager es de 30 minutos. Es posible ajustar el tiempo, o bien directamente pueden deshabilitarse los tiempos de espera de sesión.



Si se configura Access Management con las funcionalidades del lenguaje de marcado de aserción de seguridad (SAML) integradas en la cabina, es posible que se agote el tiempo de espera de sesión cuando la sesión SSO del usuario alcance su límite máximo. Esto puede ocurrir antes del tiempo de espera de sesión de System Manager.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En la sección **General**, seleccione **Habilitar/deshabilitar tiempo de espera de la sesión**.

Se abre el cuadro de diálogo **Activar/Desactivar tiempo de espera de sesión**.

3. Utilice los controles de desplazamiento para aumentar o disminuir el tiempo en minutos.

El tiempo de espera mínimo que puede configurarse para System Manager es de 15 minutos.



Para desactivar los tiempos de espera de sesiones, anule la selección de la casilla de verificación **establecer el lapso....**

4. Haga clic en **Guardar**.

Modifique la configuración de caché para la cabina de almacenamiento

Se puede ajustar la configuración de la memoria caché para el vaciado y el tamaño del bloque de todos los volúmenes de la cabina de almacenamiento.

Acerca de esta tarea

La memoria caché es un área de almacenamiento volátil temporal en la controladora que tiene un tiempo de acceso más rápido que la unidad. Para ajustar el rendimiento de la caché, se pueden modificar las siguientes opciones de configuración:

Configuración de caché	Descripción
Inicio de vaciado de caché bajo demanda	La opción Iniciar purga de caché según demanda especifica el porcentaje de datos sin escribir de la caché que activan el vaciado de caché (escritura en disco). De forma predeterminada, el vaciado de caché comienza cuando los datos sin escribir alcanzan un 80 % de la capacidad. Un porcentaje mayor es una buena opción en entornos que tienen principalmente operaciones de escritura, de manera que las solicitudes de escritura nuevas se pueden procesar mediante la caché sin tener que ir al disco. Los valores de configuración más bajos son mejores para los entornos con operaciones de I/O erráticas (con ráfagas de datos), de manera que el sistema vacía la caché con frecuencia entre las ráfagas de datos. No obstante, un porcentaje inicial inferior al 80 % puede disminuir el rendimiento.
Tamaño del bloque de caché	El tamaño de bloque de la caché determina el tamaño máximo de cada bloque de la caché, que es una unidad organizativa para la gestión de la caché. De manera predeterminada, el tamaño de bloque es de 32 KiB. System Manager permite un tamaño de bloque de caché de 4, 8, 16 o 32 KiBs. Las aplicaciones utilizan distintos tamaños de bloques, que pueden afectar al rendimiento del almacenamiento. Un tamaño menor es una buena opción para los sistemas de archivos o las aplicaciones de bases de datos. Un tamaño mayor es ideal para aplicaciones que generan operaciones de I/O secuenciales, por ejemplo, multimedia.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Desplácese hacia abajo hasta **Configuración adicional** y, a continuación, haga clic en **Cambiar configuración de caché**.

Se abre el cuadro de diálogo Cambiar configuración de caché.

3. Ajuste los siguientes valores:
 - **Iniciar purga de caché de demanda** — Seleccione un porcentaje que sea apropiado para la E/S utilizada en su entorno. Si elige un valor inferior a 80 %, es posible que note una disminución de

rendimiento.

- **Tamaño de bloque de caché** — Elija un tamaño que sea apropiado para sus aplicaciones.

4. Haga clic en **Guardar**.

Establezca la generación de informes de conectividad de host

Es posible habilitar la generación de informes de conectividad de host para que la cabina de almacenamiento supervise constantemente la conexión entre las controladoras y los hosts configurados, y emita alertas si se interrumpe la conexión. Esta función está habilitada de forma predeterminada.

Acerca de esta tarea

Si se deshabilita la generación de informes de conectividad de host, el sistema ya no supervisa la conectividad ni los problemas de los controladores multivía con un host conectado a la cabina de almacenamiento.



Al deshabilitar la generación de informes de conectividad de host, también se deshabilita el equilibrio de carga automático que supervisa y equilibra la utilización de recursos de la controladora.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Desplácese hasta **Configuración adicional** y, a continuación, haga clic en **Activar/Desactivar generación de informes de conectividad de host**.

El texto debajo de esta opción indica si se encuentra habilitada o deshabilitada.

Se abre un cuadro de diálogo de confirmación.

3. Haga clic en **Sí** para continuar.

Al seleccionar esta opción, es posible alternar entre habilitar o deshabilitar la función.

Establecer equilibrio de carga automático

La función Automatic Load Balancing garantiza que el tráfico de I/O entrante de los hosts se gestione dinámicamente y se equilibre entre ambas controladoras. Esta función está habilitada de forma predeterminada, pero se puede deshabilitar desde System Manager.

Acerca de esta tarea

Cuando la función Automatic Load Balancing está habilitada, ejecuta las siguientes funciones:

- Supervisa y equilibra automáticamente la utilización de recursos de la controladora.
- Ajusta automáticamente la propiedad de la controladora de volumen cuando es necesario y así, optimiza el ancho de banda de I/O entre los hosts y la cabina de almacenamiento.

Puede ser conveniente deshabilitar Automatic Load Balancing en la cabina de almacenamiento por las siguientes razones:

- No se desea cambiar automáticamente la propiedad de una controladora de volumen para equilibrar la carga de trabajo.

- Se trabaja en un entorno altamente optimizado donde la distribución de carga se configura intencionalmente para lograr una distribución específica entre las controladoras.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Desplácese hasta **Configuración adicional** y, a continuación, haga clic en **Habilitar/deshabilitar equilibrio de carga automático**.

El texto debajo de esta opción indica si la función se encuentra habilitada o deshabilitada.

Se abre un cuadro de diálogo de confirmación.

3. Confirme haciendo clic en **Sí** para continuar.

Al seleccionar esta opción, es posible alternar entre habilitar o deshabilitar la función.



Cuando esta función pasa de estar deshabilitada a habilitada, también se habilita la función Host Connectivity Reporting.

Cambiar el tipo de host predeterminado

Use la opción de configuración Cambiar el sistema operativo del host predeterminado para cambiar el tipo de host predeterminado en el nivel de la cabina de almacenamiento. En general, se debe cambiar el tipo de host predeterminado antes de conectar hosts a la cabina de almacenamiento o al añadir hosts adicionales.

Acerca de esta tarea

Tenga en cuenta estas directrices:

- Si todos los hosts que piensa conectar a la cabina de almacenamiento tienen el mismo sistema operativo (entorno de host homogéneo), cambie el tipo de host para que coincida con el sistema operativo.
- Si hay hosts con diferentes sistemas operativos que piensa conectar a la cabina de almacenamiento (entorno de host heterogéneo), cambie el tipo de host para que coincida con la mayoría de los sistemas operativos de los hosts.

Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y seis de ellos tienen un sistema operativo Windows, debe seleccionar Windows como tipo de sistema operativo de host predeterminado.

- Si la mayoría de los hosts conectados poseen una combinación de sistemas operativos diferentes, cambie el tipo de host a opción predeterminada de fábrica.

Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y dos de ellos tienen un sistema operativo Windows, tres ejecutan un sistema operativo VMware, Y otros tres ejecutan un sistema operativo Linux, debe seleccionar opción predeterminada de fábrica como el tipo de sistema operativo del host predeterminado.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Desplácese hasta **Configuración adicional** y, a continuación, haga clic en **Cambiar el tipo de sistema operativo del host** predeterminado.

3. Seleccione el tipo de sistema operativo de host que desea usar como predeterminado.
4. Haga clic en **Cambiar**.

Habilitar o deshabilitar la interfaz de gestión heredada

Es posible habilitar o deshabilitar la interfaz de gestión heredada (Symbol), que es un método de comunicación entre la cabina de almacenamiento y el cliente de gestión.

Acerca de esta tarea

De manera predeterminada, la interfaz de gestión heredada está activada. Si se desactiva, la cabina de almacenamiento y su cliente de gestión utilizan un método más seguro de comunicación (API DE REST a través de https); sin embargo, ciertas herramientas y tareas pueden verse afectadas si se deshabilita la cabina.



Para el sistema de almacenamiento EF600, esta función está deshabilitada de manera predeterminada.

La configuración afecta a las operaciones de la siguiente manera:

- **Activado** (predeterminado) — Configuración necesaria para configurar la duplicación con la CLI y otras herramientas, como el adaptador OCI.
- **Off** — Configuración requerida para reforzar la confidencialidad en las comunicaciones entre la matriz de almacenamiento y el cliente de administración, y para acceder a herramientas externas. Opción recomendada para configurar un servidor de directorio (LDAP).

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Desplácese hacia abajo hasta **Configuración adicional** y, a continuación, haga clic en **Cambiar interfaz de administración**.
3. En el cuadro de diálogo, haga clic en **Sí** para continuar.

Preguntas frecuentes

¿Qué es la caché de la controladora?

La caché de la controladora es un espacio de memoria física que optimiza dos tipos de operaciones de I/O (entrada/salida): Entre las controladoras y los hosts, y entre las controladoras y los discos.

En el caso de las transferencias de datos de lectura y escritura, los hosts y las controladoras se comunican a través de conexiones de alta velocidad. Sin embargo, la comunicación del back-end de la controladora a los discos es más lenta debido a que los discos son dispositivos relativamente lentos.

Cuando la caché de la controladora recibe los datos, la controladora reconoce qué aplicaciones host son las que ahora tienen los datos. De este modo, las aplicaciones host no necesitan esperar a que se escriban las operaciones de I/O en el disco. En cambio, las aplicaciones pueden continuar con sus operaciones. Los datos en caché también están a disposición de las aplicaciones de servidor, lo que elimina la necesidad de lecturas adicionales del disco para acceder a los datos.

La caché de la controladora afecta al rendimiento general de la cabina de almacenamiento de diversas

maneras:

- La caché actúa como un búfer, de modo que las transferencias de datos entre disco y host no necesitan sincronizarse.
- Los datos de una operación de escritura o lectura del host pueden estar en caché desde una operación anterior, lo que elimina la necesidad de acceder al disco.
- Si se utiliza el almacenamiento en caché de escritura, el host puede enviar comandos de escritura posteriores antes de que los datos de una operación de escritura anterior se escriban en el disco.
- Si la captura previa de caché está habilitada, el acceso de lectura secuencial se optimiza. La captura previa de caché hace que una operación de lectura tenga más probabilidades de encontrar los datos en la caché, en lugar de leer los datos del disco.



Posible pérdida de datos — Si activa la opción **almacenamiento en caché de escritura sin baterías** y no dispone de una fuente de alimentación universal de protección, podría perder datos. Además, puede perder datos si no tiene baterías de controlador y activa la opción **almacenamiento en caché de escritura sin baterías**.

¿Qué es el vaciado de la caché?

Cuando la cantidad de datos no guardados que se encuentra en la caché llega a cierto nivel, la controladora guarda periódicamente en una unidad los datos en caché. Este proceso de guardado se denomina "vaciado".

La controladora utiliza dos algoritmos para vaciar la caché: En función de la demanda y en función de la antigüedad. La controladora utiliza un algoritmo en función de la demanda hasta que la cantidad de datos en caché desciende por debajo del umbral de vaciado de caché. De manera predeterminada, un vaciado comienza cuando está en uso el 80 % de la caché.

En System Manager, puede configurar el umbral «Iniciar purga de caché a demanda» para que admita mejor el tipo de I/O utilizado en su entorno. En un entorno principalmente compuesto por operaciones de escritura, debe establecer un porcentaje alto de «Iniciar purga de caché a demanda» para aumentar la probabilidad de que cualquier solicitud de escritura nueva se pueda procesar mediante la caché sin tener que ir al disco. La configuración de un porcentaje alto limita la cantidad de vaciados de caché a fin de que más datos permanezcan en la caché, lo que aumenta la posibilidad de más aciertos en caché.

En un entorno en el que las operaciones de I/O son erráticas (con picos de datos), es posible utilizar un vaciado de caché bajo para que el sistema vacíe la caché con frecuencia entre los picos de datos. En un entorno diverso de operaciones de I/O que procesa diferentes cargas, o cuando se desconoce el tipo de cargas, se puede configurar un umbral del 50 % como un buen punto de partida intermedio. Tenga en cuenta que, si selecciona un porcentaje de inicio inferior al 80 %, es posible que disminuya el rendimiento, ya que los datos necesarios para la lectura del host pueden no estar disponibles. Además, un porcentaje más bajo también aumenta la cantidad de escrituras de disco necesarias para mantener el nivel de caché, lo que aumenta la sobrecarga del sistema.

El algoritmo en función de la antigüedad especifica el periodo durante el cual los datos de escritura pueden permanecer en la caché antes de calificar para el vaciamiento a los discos. Las controladoras utilizan el algoritmo en función de la antigüedad hasta que se alcanza el umbral de vaciado de caché. El valor predeterminado es de 10 segundos, pero este lapso se considera solo en periodos de inactividad. No puede modificar el tiempo de vaciado en System Manager; en su lugar, debe utilizar el comando **Set Storage Array** en la interfaz de línea de comandos (CLI).



Posible pérdida de datos — Si activa la opción **almacenamiento en caché de escritura sin baterías** y no dispone de una fuente de alimentación universal de protección, podría perder datos. Además, puede perder datos si no tiene baterías de controlador y activa la opción **almacenamiento en caché de escritura sin baterías**.

¿Qué es el tamaño de bloque de caché?

La controladora de la cabina de almacenamiento organiza su caché en "bloques", que son fragmentos de memoria que pueden tener un tamaño de 8, 16 o 32 KiB. Todos los volúmenes del sistema de almacenamiento comparten el mismo espacio de caché; por lo tanto, los volúmenes solo pueden tener un tamaño de bloque de caché.

Las aplicaciones utilizan diferentes tamaños de bloque, lo que puede afectar el rendimiento del almacenamiento. De manera predeterminada, el tamaño de bloque en System Manager es de 32 KiB, pero se puede modificar el valor a 8, 16 o 32 KiB. Un tamaño menor es una buena opción para los sistemas de archivos o las aplicaciones de bases de datos. Un tamaño mayor es una buena opción para aplicaciones que requieren grandes transferencias de datos, operaciones de I/O secuenciales o alto ancho de banda, como las aplicaciones multimedia.

¿Cuándo se deben sincronizar los relojes de la cabina de almacenamiento?

Se deben sincronizar manualmente los relojes de las controladoras en la cabina de almacenamiento si se observa que las marcas de tiempo que se muestran en System Manager no están alineadas con las marcas de tiempo del cliente de gestión (el ordenador que accede a System Manager por medio del explorador). Esta tarea es necesaria solo si no se habilitó el protocolo de tiempo de redes (NTP) en System Manager.



Se recomienda enfáticamente utilizar un servidor NTP en lugar de sincronizar manualmente los relojes. NTP sincroniza automáticamente los relojes con un servidor externo que utiliza el protocolo de tiempo de redes simple (SNTP).

Se puede comprobar el estado de sincronización desde el cuadro de diálogo Sincronizar relojes de cabinas de almacenamiento, que se encuentra disponible en la página sistema. Si las horas que aparecen en el cuadro de diálogo no coinciden, ejecute una sincronización. Puede ver este cuadro de diálogo periódicamente y verificar si las horas que muestran los relojes de las controladoras se distanciaron y ya no están sincronizadas.

¿Qué es la generación de informes de conectividad de host?

Cuando la opción de generación de informes de conectividad de host está habilitada, la cabina de almacenamiento supervisa continuamente la conexión entre las controladoras y los hosts configurados, y luego notifica si se interrumpió la conexión.

Pueden producirse interrupciones en la conexión si hay algún cable suelto, dañado o faltante, o si hay otro problema con el host. En estas situaciones, es posible que el sistema abra un mensaje de Recovery Guru:

- **Pérdida de redundancia del host** — se abre si alguno de los controladores no puede comunicarse con el host.
- **Tipo de host incorrecto** — se abre si el tipo de host se ha especificado incorrectamente en la matriz de

almacenamiento, lo que podría dar lugar a problemas de conmutación por error.

Puede ser conveniente deshabilitar la generación de informes de conectividad de host cuando la operación de reinicio de una controladora puede demorar más que el tiempo de espera de conexión. Cuando se deshabilita esta función, se suprimen los mensajes de Recovery Guru.



Además, al deshabilitar la generación de informes de conectividad de host también se deshabilita el equilibrio de carga automático, que supervisa y equilibra el uso de recursos de la controladora. Sin embargo, si se vuelve a habilitar la generación de informes de conectividad de host, la función de equilibrio de carga automático no se vuelve a habilitar automáticamente.

Sistema: Configuración de iSCSI

Conceptos

Terminología de iSCSI

Conozca la forma en que los términos de iSCSI se aplican a su cabina de almacenamiento.

Duración	Descripción
CHAP	El método de protocolo de autenticación por desafío mutuo (CHAP) valida la identidad de destinos e iniciadores durante el enlace inicial. La autenticación se basa en una clave de seguridad compartida denominada CHAPsecret__.
Controladora	Una controladora consta de una placa, un firmware y un software. Controla las unidades e implementa las funciones de System Manager.
DHCP	El protocolo de configuración dinámica de hosts (DHCP) es un protocolo que se usa en las redes de protocolo de Internet (IP) para los parámetros de configuración de red de distribución dinámica, como las direcciones IP.
IB	InfiniBand (IB) es una norma de comunicación para la transmisión de datos entre servidores de alto rendimiento y sistemas de almacenamiento.
Respuesta ICMP PING	El protocolo de mensajes de control de Internet (ICMP) es un protocolo que usan los sistemas operativos de ordenadores conectados a una red para enviar mensajes. Los mensajes ICMP determinan si se puede acceder a un host y cuánto tiempo lleva trasladar paquetes desde o hacia ese host.
IQN	Un identificador de nombre completo de iSCSI (IQN) es un nombre único para un iniciador de iSCSI o un destino iSCSI.
Iser	Las extensiones de iSCSI para RDMA (Iser) conforman un protocolo que extiende el protocolo iSCSI para operaciones a través de transporte RDMA, como InfiniBand o Ethernet.

Duración	Descripción
ISNS	El servicio de nombres de almacenamiento de Internet (iSNS) es un protocolo que permite la detección, gestión y configuración automatizada de dispositivos iSCSI y Fibre Channel en redes TCP/IP.
Dirección MAC	Ethernet utiliza identificadores de control de acceso de medios (direcciones MAC) para distinguir entre canales lógicos distintos que conectan dos puertos en la misma interfaz de red de transporte físico.
Cliente de gestión	Un cliente de gestión es el equipo donde se instala un explorador para acceder a System Manager.
MTU	Una unidad de transmisión máxima (MTU) es el paquete o el marco de mayor tamaño que se pueden enviar en una red.
RDMA	El acceso directo a memoria remota (RDMA) es una tecnología que les permite a los equipos en red intercambiar datos en la memoria principal sin la participación del sistema operativo de ninguno de los equipos.
Sesión de detección sin nombre	Cuando se habilita la opción de sesiones de detección sin nombre, no se requiere que los iniciadores de iSCSI especifiquen el IQN objetivo para recuperar la información de la controladora.

Procedimientos

Configure los puertos iSCSI

Si la controladora incluye una conexión de host iSCSI, los ajustes del puerto iSCSI se pueden configurar desde la página sistema.

Antes de empezar

- La controladora debe incluir puertos iSCSI; de lo contrario, la configuración de iSCSI no estará disponible.
- Se debe conocer la velocidad de la red (la tasa de transferencia de datos entre los puertos y el host).



La configuración y las funciones iSCSI solamente aparecen si la cabina de almacenamiento es compatible con iSCSI.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Configuración iSCSI**, seleccione **Configurar puertos iSCSI**.




La opción **Configurar puertos iSCSI** aparece sólo si System Manager detecta puertos iSCSI en la controladora.

3. Seleccione la controladora con los puertos iSCSI que desea configurar.
4. En la lista desplegable, seleccione el puerto que desea configurar y, a continuación, haga clic en **Siguiente**.

5. Seleccione los valores del puerto de configuración y, a continuación, haga clic en **Siguiente**.

Para ver todas las configuraciones de puerto, haga clic en el enlace **Mostrar más opciones de puerto** situado a la derecha del cuadro de diálogo.

Detalles del campo

Opción de configuración de puertos	Descripción
Habilite IPv4/Habilitar IPv6	<p>Seleccione una o ambas opciones para habilitar la compatibilidad con las redes IPv4 e IPv6.</p> <div> Si desea deshabilitar el acceso al puerto, cancele la selección de las dos casillas de comprobación.</div>
Puerto de escucha TCP (disponible haciendo clic en Mostrar más opciones de puerto).	<p>De ser necesario, introduzca un nuevo número de puerto.</p> <p>El puerto de escucha es el número de puerto TCP que la controladora utiliza para escuchar inicios de sesión iSCSI de iniciadores iSCSI del host. El puerto de escucha predeterminado es 3260. Debe introducir 3260 o un valor entre 49 49152 y 65 65535.</p>
Tamaño de MTU (disponible haciendo clic en Mostrar más opciones de puerto).	<p>De ser necesario, introduzca un nuevo tamaño en bytes para la unidad de transmisión máxima (MTU).</p> <p>El tamaño de MTU predeterminado es de 1500 bytes por trama. Debe introducir un valor entre 1500 y 9000.</p>
Habilite las respuestas PING de ICMP PING	<p>Seleccione esta opción para habilitar el protocolo de mensajes de control de Internet (ICMP). Los sistemas operativos de equipos en red usan ese protocolo para enviar mensajes. Esos mensajes ICMP determinan si es posible acceder a un host y cuánto tiempo debe transcurrir para enviar y recibir los paquetes de ese host.</p>

Si seleccionó **Activar IPv4**, se abre un cuadro de diálogo para seleccionar la configuración IPv4 después de hacer clic en **Siguiente**. Si seleccionó **Activar IPv6**, se abre un cuadro de diálogo para seleccionar la configuración de IPv6 después de hacer clic en **Siguiente**. Si seleccionó ambas opciones, primero se abre el cuadro de diálogo de configuración IPv4 y después de hacer clic en **Siguiente**, se abre el cuadro de diálogo de configuración de IPv6.

6. Configure los valores para IPv4 o IPv6 de forma automática o manual. Para ver todas las opciones de configuración de puertos, haga clic en el enlace **Mostrar más valores** situado a la derecha del cuadro de diálogo.

Detalles del campo

Opción de configuración de puertos	Descripción
Obtener configuración automáticamente	Seleccione esta opción para obtener automáticamente la configuración.
Especificar manualmente la configuración estática	Seleccione esta opción e introduzca una dirección estática en los campos. (Si lo desea, puede cortar y pegar direcciones en los campos.) En el caso de IPv4, incluya la máscara de subred y la puerta de enlace. En el caso de IPv6, incluya la dirección IP enrutable y la dirección IP del enrutador.
Active la compatibilidad con VLAN (disponible haciendo clic en Mostrar más opciones).	Seleccione esta opción para habilitar una VLAN e introducir su ID. Una red de área local virtual (VLAN) es una red lógica que se comporta como si estuviese físicamente separada de otras redes de área local virtuales y físicas (LAN) admitidas por los mismos switches, los mismos enrutadores, o ambos.
Activar prioridad ethernet (disponible haciendo clic en Mostrar más valores).	<p>Seleccione esta opción para habilitar el parámetro que determina la prioridad de acceso a la red. Use la barra deslizante para seleccionar una prioridad entre 1 (más baja) y 7 (más alta).</p> <p>En un entorno de red de área local (LAN) compartida, como Ethernet, es posible que muchas estaciones compitan por el acceso a la red. El acceso se otorga por orden de llegada. Es posible que dos estaciones intenten acceder a la red al mismo tiempo, lo que provoca que ambas estaciones se apaguen y esperen antes de volver a intentarlo. Este proceso se minimiza para Ethernet con switch, donde existe una sola estación conectada a un puerto del switch.</p>

7. Haga clic en **Finalizar**.

Configure la autenticación iSCSI

Para obtener seguridad adicional en una red iSCSI, se puede establecer la autenticación entre controladoras (objetivos) y hosts (iniciadores). System Manager usa el método de protocolo de autenticación por desafío mutuo (CHAP), que valida la identidad de los destinos e iniciadores durante el enlace inicial. La autenticación se basa en una clave de seguridad compartida denominada CHAP *secret* _.

Antes de empezar

Es posible establecer el secreto CHAP para los iniciadores (hosts iSCSI) antes o después de haber establecido el secreto CHAP para los objetivos (controladoras). Antes de seguir las instrucciones de esta tarea, primero debe esperar a que los hosts hayan establecido una conexión iSCSI y, a continuación, configurar el secreto CHAP en los hosts individuales. Una vez realizadas las conexiones, los nombres IQN de los hosts y los secretos CHAP se enumeran en el cuadro de diálogo de autenticación iSCSI (que se describe en esta tarea), y no es necesario introducirlos manualmente.

Acerca de esta tarea

Se puede seleccionar uno de los siguientes métodos de autenticación:

- **Autenticación unidireccional** — Utilice esta opción para permitir que el controlador autentique la identidad de los hosts iSCSI (autenticación unidireccional).
- **Autenticación bidireccional** — Utilice este ajuste para permitir que tanto el controlador como los hosts iSCSI lleven a cabo la autenticación (autenticación bidireccional). Esta opción aporta un segundo nivel de seguridad, ya que permite que la controladora autentique la identidad de los hosts iSCSI y, a su vez, que los hosts iSCSI autentiquen la identidad de la controladora.



La configuración y las funciones de iSCSI solo aparecen en la página Configuración si la cabina de almacenamiento es compatible con iSCSI.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Configuración de iSCSI**, haga clic en **Configurar autenticación**.

Aparece el cuadro de diálogo **Configurar autenticación**, que muestra el método actualmente establecido. También muestra si alguno de los hosts tiene secretos CHAP configurados.

3. Seleccione una de las siguientes opciones:
 - **Sin autenticación** — Si no desea que el controlador autentique la identidad de los hosts iSCSI, seleccione esta opción y haga clic en **Finalizar**. El cuadro de diálogo se cierra y la configuración está lista.
 - **Autenticación unidireccional** — para permitir que el controlador autentique la identidad de los hosts iSCSI, seleccione esta opción y haga clic en **Siguiente** para abrir el cuadro de diálogo Configurar CHAP de destino.
 - **Autenticación bidireccional** — para permitir que tanto el controlador como los hosts iSCSI lleven a cabo la autenticación, seleccione esta opción y haga clic en **Siguiente** para abrir el cuadro de diálogo Configurar CHAP de destino.
4. Tanto para la autenticación unidireccional como para la bidireccional, introduzca o confirme el secreto CHAP de la controladora (el objetivo). El secreto CHAP debe tener entre 12 y 57 caracteres ASCII imprimibles.



Si el secreto CHAP de la controladora se configuró anteriormente, los caracteres que aparecen en el campo se muestran enmascarados. Si es necesario, puede reemplazar los caracteres existentes (los caracteres nuevos no están enmascarados).

5. Debe realizar una de las siguientes acciones:
 - Si está configurando la autenticación *unidireccional*, haga clic en **Finalizar**. El cuadro de diálogo se cierra y la configuración está lista.
 - Si está configurando la autenticación *bidireccional*, haga clic en **Siguiente** para abrir el cuadro de diálogo Configurar CHAP del iniciador.
6. En el caso de la autenticación bidireccional, introduzca o confirme un secreto CHAP de cualquiera de los hosts iSCSI (los iniciadores), que pueden tener entre 12 y 57 caracteres ASCII imprimibles. Si no desea configurar la autenticación bidireccional para un host en particular, deje en blanco el campo **Secreto CHAP del iniciador**.



Si el secreto CHAP de un host se configuró con anterioridad, los caracteres del campo están enmascarados. Si es necesario, puede reemplazar los caracteres existentes (los caracteres nuevos no están enmascarados).

7. Haga clic en **Finalizar**.

Resultados

La autenticación sucede durante la secuencia de inicio de sesión iSCSI, entre las controladoras y los hosts iSCSI, a menos que no se haya especificado ninguna autenticación.

Habilite la configuración de detección de iSCSI

Es posible habilitar la configuración relacionada con la detección de dispositivos de almacenamiento en una red iSCSI. La configuración de detección de objetivos permite registrar la información de iSCSI de la cabina de almacenamiento con el protocolo de servicio de nombres de almacenamiento de Internet (iSNS), y también determinar si se deben permitir las sesiones de detección sin nombre.

Antes de empezar

Si el servidor iSNS utiliza una dirección IP estática, esa dirección debe estar disponible para registrarse en iSNS. Se admiten tanto IPv4 como IPv6.

Acerca de esta tarea

Es posible habilitar la siguiente configuración relacionada con la detección de iSCSI:

- **Activar el servidor iSNS para registrar un destino** — cuando está activado, la cabina de almacenamiento registra la información de su nombre completo iSCSI (IQN) y su puerto del servidor iSNS. Esta opción permite la detección de iSNS para que un iniciador pueda recuperar la información de IQN y puerto del servidor iSNS.
- **Activar sesiones de detección sin nombre** — cuando las sesiones de detección sin nombre están habilitadas, el iniciador (host iSCSI) no necesita proporcionar el IQN del destino (controladora) durante la secuencia de inicio de sesión para una conexión de tipo de detección. Cuando se deshabilitan, los hosts deben proporcionar el IQN para establecer una sesión de detección con la controladora. Sin embargo, siempre se requiere el IQN objetivo durante una sesión normal (con I/O). Al deshabilitar esta opción, se puede evitar que los hosts iSCSI no autorizados se conecten a la controladora mediante esta dirección IP solamente.



La configuración y las funciones de iSCSI solo aparecen en la página Configuración si la cabina de almacenamiento es compatible con iSCSI.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Configuración de iSCSI**, haga clic en **Ver/editar configuración de detección de objetivos**.

Aparece el cuadro de diálogo **Configuración de detección de objetivos**. Debajo del **Activar servidor iSNS...** campo, el cuadro de diálogo indica si la controladora ya está registrada.

3. Para registrar el controlador, seleccione **Activar servidor iSNS para registrar mi destino** y, a continuación, seleccione una de las siguientes opciones:
 - **Obtener automáticamente la configuración del servidor DHCP** — Seleccione esta opción si desea

configurar el servidor iSNS usando un servidor DHCP (Dynamic Host Configuration Protocol). Tenga en cuenta que, si usa esta opción, todos los puertos iSCSI en la controladora también deben configurarse para usar DHCP. Si es necesario, actualice el puerto iSCSI de la controladora para habilitar esta opción.



Para que el servidor DHCP proporcione la dirección del servidor iSNS, debe configurar el servidor DHCP para que utilice la opción 43 — "Información específica del proveedor". Esta opción debe incluir la dirección IPv4 del servidor iSNS en los bytes de datos 0xa-0xd (10-13).

- **Especificar manualmente la configuración estática** — Seleccione esta opción si desea introducir una dirección IP estática para el servidor iSNS. (Si lo desea, puede cortar y pegar direcciones en los campos.) En el campo, introduzca una dirección IPv4 o IPv6. Si configuró ambas, IPv4 es la predeterminada. Introduzca además un puerto de escucha TCP (utilice 3205, que es el predeterminado, o especifique un valor entre 49 49152 y 65 65535).
4. Para permitir que la cabina de almacenamiento participe en sesiones de detección sin nombre, seleccione **Habilitar sesiones de detección sin nombre**.
- Cuando se habilita esta opción, no se requiere que los iniciadores de iSCSI especifiquen el IQN objetivo para recuperar la información de la controladora.
 - Cuando se deshabilita, se impiden las sesiones de detección a menos que el iniciador proporcione el IQN objetivo. Al deshabilitar las sesiones de detección sin nombre, se obtiene seguridad adicional.
5. Haga clic en **Guardar**.

Resultados

Se muestra una barra de progreso cuando System Manager intenta registrar la controladora en el servidor iSNS. Este proceso puede llevar hasta cinco minutos.

Ver paquetes de estadísticas de iSCSI

Es posible ver datos sobre las conexiones iSCSI con la cabina de almacenamiento.

Acerca de esta tarea

En System Manager, se muestran los siguientes tipos de estadísticas de iSCSI. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas de MAC Ethernet** — proporciona estadísticas para el control de acceso a medios (MAC). MAC también proporciona un mecanismo de direccionamiento denominado dirección física o dirección MAC. La dirección MAC es una dirección única que se asigna a cada adaptador de red. La dirección MAC ayuda a entregar paquetes de datos a un destino dentro de la subred.
- **Ethernet TCP/IP statistics** — proporciona estadísticas para TCP/IP, que es el Protocolo de control de transmisión (TCP) y el Protocolo de Internet (IP) para el dispositivo iSCSI. Con TCP, las aplicaciones en hosts en red pueden crear conexiones entre sí, mediante las cuales pueden intercambiar datos en paquetes. El IP es un protocolo orientado a datos que comunica datos por una interred conmutada por paquetes. Las estadísticas de IPv4 e IPv6 se muestran por separado.
- **Estadísticas de destino local/iniciador (protocolo)**: Muestra estadísticas para el destino iSCSI, que proporciona acceso a nivel de bloque a sus medios de almacenamiento y muestra las estadísticas de iSCSI para la matriz de almacenamiento cuando se utiliza como iniciador en operaciones de mirroring asíncrono.
- **Estadísticas de Estados operativos de DCBX** — muestra los estados operativos de las diversas funciones de Data Center Bridging Exchange (DCBX).

- **LLDP TLV statistics** — muestra las estadísticas de tipo-longitud-valor (TLV) del protocolo de detección de nivel de vínculo (LLDP).
- **Estadísticas TLV de DCBX** — muestra la información que identifica los puertos de host de la matriz de almacenamiento en un entorno de protocolo de puente del centro de datos (DCB). Esta información se comparte con los colegas de red para fines de identificación y funcionalidad.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Seleccione **Ver paquetes de estadísticas iSCSI**.
3. Haga clic en una pestaña para ver los diferentes conjuntos de estadísticas.
4. **Opcional:** para establecer la línea de base, haga clic en **establecer nueva línea de base**.

La configuración de la línea de base establece un nuevo punto de partida para la recogida de estadísticas. La misma línea de base se usa para todas las estadísticas de iSCSI.

Ver sesiones iSCSI

Es posible ver información detallada sobre las conexiones iSCSI a la cabina de almacenamiento. Se pueden realizar sesiones iSCSI con hosts o cabinas de almacenamiento remotas en una relación de reflejo asíncrono.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Seleccione **Ver/finalizar sesiones iSCSI**.

Se muestra una lista de las sesiones iSCSI actuales.

3. Para ver información adicional sobre una sesión iSCSI específica, seleccione una sesión y, a continuación, haga clic en **Ver detalles**.

Detalles del campo

Elemento	Descripción
Identificador de sesión (SSID)	La cadena hexadecimal que identifica una sesión entre un iniciador de iSCSI y un destino iSCSI. El SSID está compuesto por ISID y TPGT.
Identificador de sesión del iniciador (ISID)	La parte del iniciador del identificador de sesión. El iniciador especifica el ISID durante el inicio de sesión.
Grupo de portal de destino	El destino iSCSI.
Etiqueta del grupo de portal de destino (TPGT)	La parte del destino del identificador de sesión. Identificador numérico de 16 bits para un grupo de portales de destino iSCSI.
Nombre iSCSI del iniciador	El nombre WWN único del iniciador.
Etiqueta de iSCSI del iniciador	La etiqueta de usuario configurada en System Manager.
Alias del iniciador de iSCSI	Un nombre que también puede asociarse a un nodo iSCSI. El alias permite a una organización asociar una cadena intuitiva al nombre iSCSI. Sin embargo, el alias no es un sustituto del nombre iSCSI. El alias del iniciador de iSCSI solo puede configurarse en el host, no en System Manager
Host	El servidor que envía entrada y salida a la cabina de almacenamiento.
Identificador de conexión (CID)	Nombre único para una conexión dentro de la sesión entre el iniciador y el destino. El iniciador genera este ID y lo presenta al destino durante las solicitudes de inicio de sesión. El ID de conexión también se presenta durante los cierres de sesión que cierran las conexiones.
Identificador de puerto Ethernet	El puerto de la controladora asociado a la conexión.
Dirección IP del iniciador	La dirección IP del iniciador.
Parámetros de inicio de sesión negociados	Los parámetros que se negocian durante el inicio de sesión de la sesión iSCSI.
Método de autenticación	La técnica para autenticar usuarios que desean acceder a la red iSCSI. Los valores válidos son CHAP y Ninguno .

Elemento	Descripción
Método de resumen del encabezado	La técnica para mostrar posibles valores de encabezados para la sesión iSCSI. HeaderDigest y DataDigest pueden ser None o CRC32C . El valor predeterminado para ambos es Ninguno .
Método de resumen de datos	La técnica para mostrar posibles valores de datos para la sesión iSCSI. HeaderDigest y DataDigest pueden ser None o CRC32C . El valor predeterminado para ambos es Ninguno .
Conexiones máximas	El mayor número de conexiones permitidas para la sesión iSCSI. El número máximo de conexiones puede ser de 1 a 4. El valor predeterminado es 1 .
Alias de destino	La etiqueta asociada al destino.
Alias del iniciador	La etiqueta asociada al iniciador.
Dirección IP de destino	La dirección IP del destino para la sesión iSCSI. Los nombres DNS no son compatibles.
R2T inicial	La inicial lista para transferir Estados. El estado puede ser Sí o no .
Longitud de ráfaga máxima	La carga útil máxima de SCSI en bytes para esta sesión iSCSI. La longitud máxima de ráfaga puede ser de 512 a 262,144 144 (256 KB). El valor predeterminado es 262,144 (256 KB) .
Longitud de la primera ráfaga	La carga útil de SCSI en bytes para datos no solicitados para esta sesión iSCSI. La longitud de la primera ráfaga puede ser de 512 a 131,072 072 (128 KB). El valor predeterminado es 65,536 (64 KB) .
Tiempo predeterminado de espera	La cantidad mínima de segundos que se deben esperar para intentar establecer una conexión después de la terminación o el restablecimiento de una conexión. El valor predeterminado de tiempo para esperar puede ser de 0 a 3600. El valor predeterminado es 2 .
Tiempo predeterminado de retención	La cantidad máxima de segundos durante los cuales aún puede establecerse una conexión después de la terminación o el restablecimiento de una conexión. El valor predeterminado de tiempo para retener puede ser de 0 a 3600. El valor predeterminado es 20 .
R2T pendiente máximo	La cantidad máxima de Estados listos para transferencia pendientes para esta sesión iSCSI. El valor máximo de Estados listos para transferencia pendientes puede ser de 1 a 16. El valor predeterminado es 1 .
Nivel de recuperación de errores	El nivel de recuperación de error para esta sesión iSCSI. El valor del nivel de recuperación de errores siempre está establecido en 0 .

Elemento	Descripción
Longitud máxima del segmento de datos de recepción	La cantidad máxima de datos que el iniciador o el destino pueden recibir en cualquier unidad de datos de carga útil de iSCSI (PDU).
Nombre de destino	El nombre oficial del destino (no el alias). El nombre de destino con formato <i>IQN</i> .
Nombre del iniciador	El nombre oficial del iniciador (no el alias). El nombre del iniciador que usa formato <i>IQN</i> o <i>eui</i> .

4. **Opcional:** para guardar el informe en un archivo, haga clic en **Guardar**.

El archivo se guarda en la carpeta de descargas del explorador con el nombre de archivo `iscsi-session-connections.txt`.

Finalice la sesión iSCSI

Es posible finalizar una sesión iSCSI que no se necesita. Se pueden realizar sesiones iSCSI con hosts o cabinas de almacenamiento remotas en una relación de reflejo asíncrono.

Acerca de esta tarea

Es posible que desee finalizar una sesión iSCSI por los siguientes motivos:

- **Acceso no autorizado** — Si un iniciador iSCSI está conectado y no debe tener acceso, puede finalizar la sesión iSCSI para forzar al iniciador iSCSI fuera de la matriz de almacenamiento. El iniciador de iSCSI puede haber iniciado sesión porque el método de autenticación Ninguno estaba disponible.
- **Tiempo de inactividad del sistema** — Si necesita desconectar una matriz de almacenamiento y observa que los iniciadores iSCSI todavía están conectados, puede finalizar las sesiones iSCSI para sacar los iniciadores iSCSI de la matriz de almacenamiento.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Seleccione **Ver/finalizar sesiones iSCSI**.

Se muestra una lista de las sesiones iSCSI actuales.

3. Seleccione la sesión que desea finalizar
4. Haga clic en **Finalizar sesión** y confirme que desea realizar la operación.

Configure los puertos Iser over InfiniBand

Si la controladora tiene un puerto Iser over InfiniBand, se puede configurar la conexión de red al host.

Antes de empezar

- La controladora debe tener un puerto Iser over InfiniBand; de lo contrario, las opciones de Iser over InfiniBand no estarán disponibles en System Manager.
- Se debe conocer la dirección IP de la conexión de host.

Pasos

1. Seleccione **MENU:Settings[System]**
2. En **Configuración de Iser over InfiniBand**, seleccione **Configurar puertos Iser over InfiniBand**.
3. Haga clic en la controladora que tenga el puerto Iser over InfiniBand que desea configurar. Haga clic en **Siguiente**.
4. En el menú desplegable, seleccione el puerto HIC que desea configurar y después introduzca la dirección IP del host.
5. Haga clic en **Finalizar**.
6. Restablezca el puerto Iser over InfiniBand. Para ello, haga clic en **Sí**.

Ver estadísticas de Iser over InfiniBand

Si la controladora de la cabina de almacenamiento incluye un puerto Iser over InfiniBand, es posible ver datos sobre las conexiones del host.

Acerca de esta tarea

En System Manager, se muestran los siguientes tipos de estadísticas de Iser over InfiniBand. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas de destino local (protocolo)** — proporciona estadísticas para el destino Iser over InfiniBand, que muestra el acceso de nivel de bloque a sus medios de almacenamiento.
- **Estadísticas de la interfaz Iser over InfiniBand** — proporciona estadísticas para todos los puertos Iser en la interfaz InfiniBand, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Seleccione **Ver estadísticas de Iser over InfiniBand**.
3. Haga clic en una pestaña para ver los diferentes conjuntos de estadísticas.
4. **Opcional:** para establecer la línea de base, haga clic en **establecer nueva línea de base**.

La configuración de la línea de base establece un nuevo punto de partida para la recogida de estadísticas. La misma línea de base se usa para todas las estadísticas de Iser over InfiniBand.

Preguntas frecuentes

¿Qué sucede cuando utilizo un servidor iSNS para el registro?

Cuando se utiliza información del servidor de servicio de nombres de almacenamiento de

Internet (iSNS), los hosts (iniciadores) pueden configurarse para consultar el servidor iSNS a fin de recuperar información del objetivo (controladoras).

Este registro proporciona al servidor iSNS la información del puerto y del nombre completo de iSCSI (IQN) de la controladora, y permite consultas entre los iniciadores (hosts iSCSI) y los objetivos (controladoras).

¿Qué métodos de registro se admiten automáticamente para iSCSI?

La implementación de iSCSI es compatible con el método de detección Servicio de nombres de almacenamiento de Internet (iSNS) o con el uso del comando Send Targets.

El método iSNS permite la detección iSNS entre los iniciadores (hosts iSCSI) y los objetivos (controladoras). La controladora objetivo se registra para proporcionar al servidor iSNS la información sobre el puerto y el nombre completo de iSCSI (IQN) de la controladora.

Si no se configura iSNS, el host iSCSI puede enviar el comando Send Targets durante una sesión de detección iSCSI. En respuesta, la controladora devuelve la información del puerto (por ejemplo, el IQN objetivo, la dirección IP del puerto, el puerto de escucha y el grupo de puertos de destino). Este método de detección no es necesario si utiliza iSNS, dado que el iniciador del host puede recuperar las IP objetivo del servidor iSNS.

¿Cómo se interpretan las estadísticas de Iser over InfiniBand?

El cuadro de diálogo Ver estadísticas de Iser over InfiniBand muestra las estadísticas de destino local (protocolo) y las estadísticas de la interfaz Iser over InfiniBand (IB). Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas de destino local (protocolo)** — proporciona estadísticas para el destino Iser over InfiniBand, que muestra el acceso de nivel de bloque a sus medios de almacenamiento.
- **Estadísticas de la interfaz Iser over InfiniBand** — proporciona estadísticas para todos los puertos Iser over InfiniBand en la interfaz InfiniBand, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

¿Qué más debo hacer para configurar o diagnosticar Iser over InfiniBand?

En la tabla a continuación, se enumeran las funciones de System Manager que se pueden utilizar para configurar y gestionar sesiones Iser over InfiniBand.



La configuración de Iser over InfiniBand solo está disponible si la controladora de la cabina de almacenamiento incluye un puerto de gestión de hosts Iser over InfiniBand.

Configure y diagnostique Iser over InfiniBand

Acción	Ubicación
Configure los puertos Iser over InfiniBand	<ol style="list-style-type: none"> 1. Seleccione hardware. 2. Seleccione Mostrar parte posterior de la bandeja. 3. Seleccione una controladora. 4. Seleccione Configurar puertos Iser over InfiniBand. <p>o.</p> <ol style="list-style-type: none"> 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta Configuración de Iser over InfiniBand y seleccione Configurar puertos Iser over InfiniBand.
Ver estadísticas de Iser over InfiniBand	<ol style="list-style-type: none"> 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta Configuración de Iser over InfiniBand y seleccione Ver estadísticas de Iser over InfiniBand.

Sistema: Configuración de NVMe

Conceptos

Información general de NVMe

Algunas controladoras incluyen un puerto para implementar NVMe (memoria no volátil rápida) en estructuras. NVMe permite una comunicación de alto rendimiento entre los hosts y la cabina de almacenamiento.

¿Qué es NVMe?

NVM significa "memoria no volátil", y es una memoria persistente utilizada en muchos tipos de dispositivos de almacenamiento. NVMe (NVM Express) es una interfaz o un protocolo estandarizados diseñados específicamente para la comunicación de varias colas de alto rendimiento con dispositivos NVM.

¿Qué es NVMe over Fabrics?

NVMe over Fabrics (NVMe-of) es una especificación de tecnología que permite la transferencia de datos y comandos basados en mensajes de NVMe entre un equipo host y un almacenamiento a través de una red. Un host puede acceder a una cabina de almacenamiento NVMe (que se denomina *SUBSYSTEM*) con una estructura. Los comandos NVMe se habilitan y se encapsulan en capas de abstracción de transporte en el lado del host y del subsistema. Esto extiende la interfaz NVMe integral de alto rendimiento desde el host hasta el almacenamiento, además de estandarizar y simplificar el conjunto de comandos.

El almacenamiento NVMe-of se presenta a un host como dispositivo de almacenamiento basado en bloques local. El volumen (que se denomina *Namespace*) puede montarse en un sistema de archivos, como sucede con cualquier otro dispositivo de almacenamiento en bloques. Es posible usar la API de REST, la SMcli o SANtricity System Manager para aprovisionar el almacenamiento según sea necesario.

¿Qué es un nombre completo de NVMe (NQN)?

El nombre completo de NVMe (NQN) se utiliza para identificar el destino de almacenamiento remoto. El nombre completo de NVMe para la cabina de almacenamiento siempre es una asignación del subsistema que no puede modificarse. Hay un solo nombre completo de NVMe para toda la cabina. El nombre completo de NVMe se limita a 223 caracteres de longitud. Es posible compararlo con un nombre completo de iSCSI.

¿Qué es un espacio de nombres y un identificador de espacio de nombres?

Un espacio de nombres es el equivalente a una unidad lógica en SCSI, que está relacionada con un volumen en la cabina. El identificador de espacio de nombres (NSID) es equivalente a un número de unidad lógica (LUN) en SCSI. Es posible crear el NSID en el momento de la creación del espacio de nombres, y configurarlo con un valor entre 1 y 255.

¿Qué es una controladora NVMe?

Como un SCSI I_T nexus, que representa la ruta desde el iniciador del host hasta el objetivo del sistema de almacenamiento, una controladora NVMe creada durante el proceso de conexión del host ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento. Un NQN para el host más un identificador de puerto de host identifican de manera única una controladora NVMe. Si bien una controladora NVMe solo puede asociarse con un solo host, puede acceder a varios espacios de nombres.

Es posible configurar los hosts que pueden acceder a determinados espacios de nombres y configurar el identificador de espacio de nombres para el host con SANtricity System Manager. A continuación, cuando se crea la controladora NVMe, esta puede acceder a la lista de identificadores de espacio de nombres creada y utilizada para configurar las conexiones permitidas.

Terminología de NVMe

Conozca la forma en que los términos de NVMe se aplican a su cabina de almacenamiento.

Duración	Descripción
Estructura	InfiniBand (IB) es una norma de comunicación para la transmisión de datos entre servidores de alto rendimiento y sistemas de almacenamiento.
Espacio de nombres	Un espacio de nombres es almacenamiento NVM que se formateó para el acceso en bloque. Es análogo a una unidad lógica en SCSI, que se relaciona con un volumen en la cabina de almacenamiento.
Identificador de espacio de nombres	El ID del espacio de nombres es el identificador único de la controladora NVMe para el espacio de nombres y se puede configurar con un valor entre 1 y 255. Es análogo a un número de unidad lógica (LUN) en SCSI.
NQN	El nombre completo de NVMe (NQN) se utiliza para identificar el destino de almacenamiento remoto (la cabina de almacenamiento).
NVM	La memoria no volátil (NVM) es la memoria persistente utilizada en muchos tipos de dispositivos de almacenamiento.

Duración	Descripción
NVMe	La memoria no volátil rápida (NVMe) es una interfaz designada para dispositivos de almacenamiento basados en flash, por ejemplo, unidades SSD. NVMe reduce la sobrecarga de I/O e incluye mejoras de rendimiento, en comparación con las interfaces de dispositivos lógicos anteriores.
NVMe-of	La memoria no volátil rápida sobre estructuras (NVMe-of) es una especificación que permite el funcionamiento de comandos y la transferencia de datos de NVMe en una red entre un host y el almacenamiento.
Controladora NVMe	Se crea una controladora NVMe durante el proceso de conexión del host. Esta ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento.
Cola NVMe	Una cola que se utiliza para pasar comandos y mensajes a través de la interfaz de NVMe.
Subsistema NVMe	La cabina de almacenamiento con una conexión NVMe.
RDMA	El acceso remoto a memoria directa (RDMA) permite un movimiento de datos más directo hacia y desde un servidor gracias a la implementación de un protocolo de transporte en el hardware de la tarjeta de interfaz de red (NIC).
Roce	RDMA over Converged Ethernet (roce) es un protocolo de red que permite el acceso remoto a memoria directa (RDMA) sobre una red Ethernet.
SSD	Los discos de estado sólido (SSD) son dispositivos de almacenamiento de datos que usan memoria de estado sólido (flash) para almacenar datos en forma persistente. Los SSD emulan las unidades de discos duros convencionales y están disponibles con las mismas interfaces que usan las unidades de disco duro.

Procedimientos

Configure los puertos NVMe over InfiniBand

Si la controladora incluye una conexión NVMe over InfiniBand, los ajustes del puerto NVMe se pueden configurar desde la página sistema.

Antes de empezar

- La controladora debe incluir un puerto de host NVMe over InfiniBand; de lo contrario, los ajustes de NVMe over InfiniBand no estarán disponibles en System Manager.
- Se debe conocer la dirección IP de la conexión de host.



La configuración y las funciones de NVMe over InfiniBand aparecen solamente si la controladora de la cabina de almacenamiento contiene un puerto NVMe over InfiniBand.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Configuración de NVMe over InfiniBand**, seleccione **Configurar puertos NVMe over InfiniBand**.
3. Seleccione la controladora que tenga el puerto NVMe over InfiniBand que desea configurar. Haga clic en **Siguiente**.
4. Seleccione el puerto de HIC que desea configurar de la lista desplegable e introduzca la dirección IP.

Si desea configurar una cabina de almacenamiento EF600 con una HIC de 200 GB, este cuadro de diálogo muestra dos campos de dirección IP: Uno para un puerto físico (externo) y uno para un puerto virtual (interno). Debe asignar una dirección IP exclusiva a cada puerto. Estos ajustes permiten que el host establezca una ruta entre cada puerto y que la HIC alcance el rendimiento máximo. Si no se asigna una dirección IP al puerto virtual, la HIC se ejecutará a aproximadamente la mitad de su capacidad de velocidad.

5. Haga clic en **Finalizar**.
6. Restablezca el puerto NVMe over InfiniBand. Para ello, haga clic en **Sí**.

Configure los puertos NVMe over roce

Si la controladora incluye una conexión para NVMe over roce (RDMA over Converged Ethernet), es posible configurar las opciones del puerto NVMe desde la página sistema.

Antes de empezar


- La controladora debe incluir un puerto de host NVMe over roce; de lo contrario, los ajustes de NVMe over roce no estarán disponibles en System Manager.
- Se debe conocer la dirección IP de la conexión de host.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Configuración de NVMe over roce**, seleccione **Configurar puertos NVMe over roce**.
3. Seleccione la controladora que tenga el puerto NVMe over roce que desea configurar. Haga clic en **Siguiente**.
4. Seleccione el puerto de HIC que desea configurar de la lista desplegable. Haga clic en **Siguiente**.
5. Configure las opciones del puerto.

Para ver todas las configuraciones de puerto, haga clic en el enlace **Mostrar más opciones de puerto** situado a la derecha del cuadro de diálogo.

Detalles del campo

Opción de configuración de puertos	Descripción
Velocidad de puerto ethernet configurada	Seleccione la velocidad que coincida con la capacidad de velocidad del SFP en el puerto.
Habilite IPv4/Habilitar IPv6	<div>Seleccione una o ambas opciones para habilitar la compatibilidad con las redes IPv4 e IPv6.</div> <div> Si desea deshabilitar el acceso al puerto, cancele la selección de las dos casillas de comprobación.</div>
Tamaño de MTU (disponible haciendo clic en Mostrar más opciones de puerto).	<div>De ser necesario, introduzca un nuevo tamaño en bytes para la unidad de transmisión máxima (MTU).</div> <div>El tamaño de MTU predeterminado es de 1500 bytes por trama. Debe introducir un valor entre 1500 y 9000.</div>

Si seleccionó **Activar IPv4**, se abre un cuadro de diálogo para seleccionar la configuración IPv4 después de hacer clic en **Siguiente**. Si seleccionó **Activar IPv6**, se abre un cuadro de diálogo para seleccionar la configuración de IPv6 después de hacer clic en **Siguiente**. Si seleccionó ambas opciones, primero se abre el cuadro de diálogo de configuración IPv4 y después de hacer clic en **Siguiente**, se abre el cuadro de diálogo de configuración de IPv6.

1. Configure los valores para IPv4 o IPv6 de forma automática o manual.

Detalles del campo

Opción de configuración de puertos	Descripción
Obtener configuración automáticamente	Seleccione esta opción para obtener automáticamente la configuración.
Especificar manualmente la configuración estática	Seleccione esta opción e introduzca una dirección estática en los campos. (Si lo desea, puede cortar y pegar direcciones en los campos.) En el caso de IPv4, incluya la máscara de subred y la puerta de enlace. En el caso de IPv6, incluya la dirección IP enrutable y la dirección IP del enrutador. Si desea configurar una cabina de almacenamiento EF600 con una HIC de 200 GB, este cuadro de diálogo muestra dos conjuntos de campos para los parámetros de red: Uno para un puerto físico (externo) y uno para un puerto virtual (interno). Debe asignar parámetros exclusivos a cada puerto. Estos ajustes permiten que el host establezca una ruta entre cada puerto y que la HIC alcance el rendimiento máximo. Si no se asigna una dirección IP al puerto virtual, la HIC se ejecutará a aproximadamente la mitad de su capacidad de velocidad.

2. Haga clic en **Finalizar**.

Ver estadísticas de NVMe over Fabrics

Es posible ver datos acerca de las conexiones NVMe over Fabrics a la cabina de almacenamiento.

Acerca de esta tarea

En System Manager, se muestran los siguientes tipos de estadísticas de NVMe over Fabrics. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas del subsistema NVMe** — muestra estadísticas para la controladora NVMe y su cola. La controladora NVMe ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento. Es posible revisar las estadísticas del subsistema NVMe para consultar elementos, como errores de conexión, reinicios y apagados.
- **Estadísticas de la interfaz RDMA** — proporciona estadísticas para todos los puertos NVMe over Fabrics de la interfaz RDMA, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch. Esta pestaña solo se muestra cuando existen puertos NVMe over Fabrics disponibles.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. Seleccione **Ver estadísticas de NVMe over Fabrics**.

3. **Opcional:** para establecer la línea de base, haga clic en **establecer nueva línea de base**.

La configuración de la línea de base establece un nuevo punto de partida para la recogida de estadísticas. Se usa la misma línea de base para todas las estadísticas de NVMe.

Preguntas frecuentes

¿Cómo se interpretan las estadísticas de NVMe over Fabrics?

El cuadro de diálogo Ver estadísticas de NVMe over Fabrics muestra estadísticas para el subsistema NVMe y la interfaz RDMA. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas del subsistema NVMe** — muestra estadísticas para la controladora NVMe y su cola. La controladora NVMe ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento. Es posible revisar las estadísticas del subsistema NVMe para consultar elementos, como errores de conexión, reinicios y apagados. Para obtener más información sobre estas estadísticas, haga clic en **Ver leyenda de encabezados de tabla**.
- **Estadísticas de la interfaz RDMA** — proporciona estadísticas para todos los puertos NVMe over Fabrics de la interfaz RDMA, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch. Esta pestaña solo se muestra cuando existen puertos NVMe over Fabrics disponibles. Para obtener más información sobre las estadísticas, haga clic en **Ver leyenda de encabezados de tabla**.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

¿Qué más debo hacer para configurar o diagnosticar NVMe over InfiniBand?

En la tabla a continuación, se enumeran las funciones de System Manager que se pueden utilizar para configurar y gestionar sesiones NVMe over InfiniBand.



La configuración de NVMe over InfiniBand solo está disponible si la controladora de la cabina de almacenamiento incluye un puerto NVMe over InfiniBand.

Configure y diagnostique NVMe over InfiniBand

Acción	Ubicación
Configure los puertos NVMe over InfiniBand	<ol style="list-style-type: none"> 1. Seleccione hardware. 2. Seleccione Mostrar parte posterior de la bandeja. 3. Seleccione una controladora. 4. Seleccione Configurar puertos NVMe over InfiniBand. <p>o.</p> <ol style="list-style-type: none"> 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta Configuración de NVMe over InfiniBand y seleccione Configurar puertos NVMe over InfiniBand.
Ver estadísticas de NVMe over InfiniBand	<ol style="list-style-type: none"> 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta Configuración de NVMe over InfiniBand y seleccione Ver estadísticas de NVMe over Fabrics.

¿Qué más debo hacer para configurar o diagnosticar NVMe over roce?

Es posible configurar y gestionar NVMe over roce desde las páginas hardware y Configuración.



La configuración de NVMe over roce solo está disponible si la controladora de la cabina de almacenamiento incluye un puerto NVMe over roce.

Configurar y diagnosticar NVMe over roce

Acción	Ubicación
Configure los puertos NVMe over roce	<ol style="list-style-type: none"> 1. Seleccione hardware. 2. Seleccione Mostrar parte posterior de la bandeja. 3. Seleccione una controladora. 4. Seleccione Configurar puertos NVMe over roce. <p>o.</p> <ol style="list-style-type: none"> 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta Configuración de NVMe over roce y seleccione Configurar puertos NVMe over roce.
Ver estadísticas de NVMe over Fabrics	<ol style="list-style-type: none"> 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta Configuración de NVMe over roce y seleccione Ver estadísticas de NVMe over Fabrics.

¿Por qué existen dos direcciones IP para un puerto físico?

La cabina de almacenamiento EF600 puede incluir dos HIC: Una externa y una interna.

En esta configuración, la HIC externa se encuentra conectada a una HIC interna auxiliar. Cada puerto físico al que se puede obtener acceso desde la HIC externa tiene un puerto virtual asociado desde la HIC interna.

Para alcanzar el rendimiento máximo de 200 GB, es necesario asignar una dirección IP exclusiva a los puertos físico y virtual para que el host pueda establecer conexiones a ambos. Si no se asigna una dirección IP al puerto virtual, la HIC se ejecutará a aproximadamente la mitad de su capacidad de velocidad.

¿Por qué existen dos conjuntos de parámetros para un puerto físico?

La cabina de almacenamiento EF600 puede incluir dos HIC: Una externa y una interna.

En esta configuración, la HIC externa se encuentra conectada a una HIC interna auxiliar. Cada puerto físico al que se puede obtener acceso desde la HIC externa tiene un puerto virtual asociado desde la HIC interna.

Para alcanzar el rendimiento máximo de 200 GB, es necesario asignar parámetros a los puertos físico y virtual para que el host pueda establecer conexiones a ambos. Si no se asignan parámetros al puerto virtual, la HIC se ejecutará a aproximadamente la mitad de su capacidad de velocidad.

Sistema: Funciones complementarias

Conceptos

Cómo trabajar con las funciones complementarias

Las funciones adicionales son las que no se incluyen en la configuración estándar de System Manager y pueden requerir una clave para su habilitación. Una función complementaria puede ser una sola función excepcional o un paquete de funciones agrupadas.

Los siguientes pasos proporcionan información general sobre cómo habilitar una función excepcional o un paquete de funciones:

1. Obtenga la siguiente información:
 - El número de serie del chasis y el identificador de habilitación de la función, el cual identifica la cabina de almacenamiento para la función que se instalará. Estos elementos están disponibles en System Manager.
 - El código de activación de la función, que está disponible en el sitio de soporte al adquirir la función.
2. Obtenga la clave de función. Para ello, póngase en contacto con el proveedor de almacenamiento o acceda al sitio de activación de funciones premium. Proporcione el número de serie del chasis, el identificador de habilitación y el código de función para la activación.
3. En System Manager, habilite la función excepcional o el paquete de funciones con el archivo de claves de función.

Terminología de la función complementaria

Conozca la forma en que los términos de las funciones complementarias se aplican a su

cabina de almacenamiento.

Duración	Descripción
Identificador de habilitación de la función	Un identificador de habilitación de la función es una cadena única que identifica una cabina de almacenamiento específica. Este identificador garantiza que cuando se obtiene la función excepcional, esta se asocie únicamente con una cabina de almacenamiento en particular. Esta cadena aparece en la sección funciones adicionales de la página sistema.
Archivo de claves de función	Un archivo de claves de función es un archivo que se recibe para desbloquear y habilitar una función excepcional o un paquete de funciones.
Paquete de funciones	Un paquete de funciones es un paquete que cambia los atributos de la cabina de almacenamiento (por ejemplo, cambiar el protocolo Fibre Channel a iSCSI). Los paquetes de funciones requieren una clave especial para habilitarlos.
Función excepcional	Una función prémium es una opción adicional que requiere una clave para habilitarla. No se incluye en la configuración estándar de System Manager.

Procedimientos

Obtener un archivo de claves de función

Para habilitar una función excepcional o un paquete de funciones en una cabina de almacenamiento, primero es necesario obtener un archivo de claves de función. Una clave se asocia con una sola cabina de almacenamiento.

Acerca de esta tarea

En esta tarea, se describe cómo obtener la información requerida para la función y, a continuación, enviar una solicitud para un archivo de claves de función. Entre la información requerida se encuentra la siguiente:

- Número de serie del chasis
- Identificador de habilitación de la función
- Código de activación de la función

Pasos

1. En System Manager, busque y registre el número de serie del chasis. Para ver este número de serie, debe pasar el ratón por el icono Centro de soporte.
2. En System Manager, busque Identificador de habilitación de funciones. Vaya a **MENU:Settings[System]** y desplácese hacia abajo hasta **Add-ons**. Busque **Identificador de habilitación de funciones**. Registre el número de la opción Identificador de habilitación de funciones.
3. Busque y registre el código para la activación de la función. Para paquetes de funciones, este código se proporciona en las instrucciones correspondientes para realizar la conversión.

Es posible acceder a las instrucciones de NetApp en "[Centro de documentación para sistemas E-Series y EF-Series de NetApp](#)".

Para funciones excepcionales, es posible acceder al código de activación en el sitio de soporte de la

siguiente manera:

- a. Inicie sesión en ["Soporte de NetApp"](#).
 - b. Vaya a **licencias de software** para su producto.
 - c. Introduzca el número de serie del chasis de la cabina de almacenamiento y, a continuación, haga clic en **Ir**.
 - d. Busque los códigos de activación de la función en la columna **clave de licencia**.
 - e. Registre el contenido de la opción Feature Activation Code de la función deseada.
4. Para solicitar un archivo de claves de función, envíe un correo electrónico o un documento de texto al proveedor de almacenamiento con la siguiente información: Número de serie del chasis, el identificador de habilitación y el código para la activación de la función.

También puede ir a ["Activación de licencias de NetApp: Activación de funciones prémium de matriz de almacenamiento"](#) e introduzca la información requerida para obtener la función o el paquete de funciones. (Las instrucciones en este sitio son para funciones excepcionales, no paquetes de funciones.)

Después de terminar

Una vez que tenga el archivo de claves de la función, podrá habilitar la función excepcional o el paquete de funciones.

Habilite una función excepcional

Una función prémium es una opción adicional que requiere una clave para habilitarla.

Antes de empezar

- Obtuvo una clave de función. Si es necesario, comuníquese con soporte técnico para obtener una clave.
- Cargó el archivo de claves en el cliente de gestión (el sistema con un explorador para acceder a System Manager).

Acerca de esta tarea

En esta tarea, se describe cómo usar System Manager para habilitar una función excepcional.



Si desea deshabilitar una función excepcional, debe utilizar el comando Deshabilitar función de cabina de almacenamiento (`disable storageArray (featurePack | feature=featureAttributeList)`) En la interfaz de línea de comandos (CLI).

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Complementos**, seleccione **Activar característica Premium**.

Se abre el cuadro de diálogo Habilitar una función prémium.
3. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves.

El nombre del archivo aparece en el cuadro de diálogo.
4. Haga clic en **Activar**.

Habilite el paquete de funciones

Un paquete de funciones es un paquete que cambia los atributos de la cabina de almacenamiento (por ejemplo, cambiar el protocolo Fibre Channel a iSCSI). Para habilitar paquetes de funciones, se requiere una clave especial.

Antes de empezar

- Siguió las instrucciones adecuadas para realizar la conversión y preparar el sistema para los nuevos atributos de la cabina de almacenamiento.



Es posible acceder a las instrucciones de conversión en "[Centro de documentación para sistemas E-Series y EF-Series de NetApp](#)".

- La cabina de almacenamiento está sin conexión, por lo que ningún host ni aplicación accede a la cabina.
- Existen backups de todos los datos.
- Obtuvo un archivo de paquete de funciones.

El paquete de funciones está cargado en el cliente de gestión (el sistema con un explorador para acceder a System Manager).



Debe programar una ventana de mantenimiento de tiempo de inactividad y detener todas las operaciones de I/O entre el host y las controladoras. Además, tenga en cuenta que no podrá acceder a los datos en la cabina de almacenamiento hasta después de completar correctamente la conversión.

Acerca de esta tarea

En esta tarea, se describe cómo usar System Manager para habilitar un paquete de funciones. Al finalizar, debe reiniciar la cabina de almacenamiento.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Complementos**, seleccione **Cambiar paquete de funciones**.
3. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves.

El nombre del archivo aparece en el cuadro de diálogo.

4. Escriba **CHANGE** en el campo.
5. Haga clic en **Cambiar**.

Comienza la migración del paquete de funciones y se reinician las controladoras. Se eliminan los datos no escritos en la caché, lo que garantiza que no exista actividad de I/O. Las dos controladoras se reinician automáticamente para que el nuevo paquete de funciones entre en vigencia. La cabina de almacenamiento vuelve a responder cuando se completa el reinicio.

Descargar la interfaz de línea de comandos (CLI)

En System Manager, es posible descargar el paquete de la CLI. La CLI proporciona un método a partir de texto para la configuración y supervisión de cabinas. Se comunica mediante https y utiliza la misma sintaxis que la CLI que está disponible en el paquete de

software de gestión instalado de forma externa. Para descargar la CLI, no se requiere ninguna clave.

Antes de empezar

- Debe haber disponible un entorno Java Runtime Environment (JRE), versión 8 y superior en el sistema de administración en el que planea ejecutar los comandos de la CLI.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Complementos**, seleccione **interfaz de línea de comandos**.

El paquete ZIP se descargará en el explorador.

3. Guarde el archivo ZIP en el sistema de gestión donde tenga pensado ejecutar los comandos de la CLI para la cabina de almacenamiento y, a continuación, extraiga el archivo.

Ahora puede ejecutar los comandos de la CLI a partir de una solicitud del sistema operativo, como dos C: Prompt. Encontrará una referencia de comandos de la CLI en el menú Ayuda, en la parte superior derecha de la interfaz de usuario de System Manager.

Sistema: Gestión de claves de seguridad

Conceptos

Cómo opera la función Drive Security

Drive Security es una función de la cabina de almacenamiento que ofrece una capa adicional de seguridad con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security, se requiere una clave de seguridad para acceder a los datos. Cuando se retiran físicamente, las unidades de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta.

Cómo implementar Drive Security

Para implementar Drive Security, siga estos pasos.

1. Equipe la cabina de almacenamiento con unidades compatibles con la función de seguridad, ya sea con unidades FDE o FIPS. (Para los volúmenes que requieren compatibilidad con FIPS, debe utilizar únicamente unidades FIPS. Si se mezclan unidades FIPS y FDE en un grupo de volúmenes o un pool, todas las unidades se tratarán como unidades FDE. Además, una unidad FDE no puede añadirse a ni usarse como pieza de repuesto en un grupo de volúmenes o un pool completamente FIPS.)
2. Cree una clave de seguridad, que es una cadena de caracteres compartida por la controladora y las unidades para acceso de lectura/escritura. Es posible crear una clave interna desde la memoria persistente de la controladora o una clave externa desde un servidor de gestión de claves. Para la gestión de claves externas, debe establecerse una autenticación con el servidor de gestión de claves.
3. Habilite Drive Security para pools y grupos de volúmenes:
 - Cree un pool o grupo de volúmenes (busque **Sí** en la columna **compatible con la función de**

seguridad de la tabla candidatos).

- Seleccione un pool o grupo de volúmenes cuando cree un volumen nuevo (busque **Sí** junto a **compatible con la función de seguridad** en la tabla de candidatos de pools y grupos de volúmenes).

Cómo funciona Drive Security en el nivel de unidad

Una unidad compatible con la función de seguridad, FDE o FIPS, cifra los datos durante la escritura y descifra los datos durante la lectura. Estas operaciones de cifrado y descifrado no afectan al rendimiento ni al flujo de trabajo del usuario. Cada unidad tiene su propia clave de cifrado, que jamás puede transferirse de la unidad.

La función Drive Security ofrece una capa adicional de protección en unidades compatibles con la función de seguridad. Cuando se seleccionan grupos de volúmenes o pools en estas unidades para Drive Security, las unidades buscan una clave de seguridad antes de permitir el acceso a los datos. Es posible habilitar Drive Security para pools y grupos de volúmenes en cualquier momento sin afectar a los datos existentes en la unidad. Sin embargo, no es posible deshabilitar Drive Security sin borrar todos los datos en la unidad.

Cómo funciona Drive Security en el nivel de cabina de almacenamiento

Con la función Drive Security, se crea una clave de seguridad que se comparte entre las unidades con la función de seguridad habilitada y las controladoras en una cabina de almacenamiento. Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad.

Si se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento y se vuelve a instalar en otra, la unidad tendrá el estado Security Locked. La unidad reubicada busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad desde la cabina de almacenamiento de origen. Después de un proceso de desbloqueo correcto, la unidad reubicada utilizará la clave de seguridad ubicada en la cabina de almacenamiento objetivo, y el archivo de claves de seguridad importado ya no será necesario.



Para la gestión de claves internas, la clave de seguridad se almacena en una ubicación inaccesible de la controladora. No está en formato legible, y el usuario no puede acceder a ella.

Cómo funciona Drive Security en el nivel de volumen

Al crear un pool o un grupo de volúmenes desde unidades compatibles con la función de seguridad, también es posible habilitar Drive Security para estos pools o grupos de volúmenes. La opción Drive Security permite que las unidades y los pools y los grupos de volúmenes asociados tengan la función de seguridad-*enabled*.

Tenga en cuenta las siguientes directrices antes de crear pools y grupos de volúmenes con la función de seguridad habilitada:

- Los grupos de volúmenes y los pools deben estar compuestos en su totalidad por unidades compatibles con la función de seguridad. (Para los volúmenes que requieren compatibilidad con FIPS, debe utilizar únicamente unidades FIPS. Si se mezclan unidades FIPS y FDE en un grupo de volúmenes o un pool, todas las unidades se tratarán como unidades FDE. Además, una unidad FDE no puede añadirse a ni usarse como pieza de repuesto en un grupo de volúmenes o un pool completamente FIPS.)
- Los grupos de volúmenes y los pools deben tener el estado Optimal.

Cómo funciona la gestión de claves de seguridad

Cuando se implementa la función Drive Security, las unidades con la función de seguridad habilitada (FIPS o FDE) requieren una clave de seguridad para acceder a los

datos. Una clave de seguridad es una cadena de caracteres que se comparte entre estos tipos de unidades y las controladoras en una cabina de almacenamiento.

Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad. Si se elimina una unidad habilitada para seguridad de la cabina de almacenamiento, se bloquean los datos de esa unidad. Cuando se vuelve a instalar la unidad en otra cabina de almacenamiento, se busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad original.

Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos:

- Gestión de claves internas en la memoria persistente de la controladora.
- Gestión de claves externas en un servidor de gestión de claves externo.

Gestión de claves internas

Las claves internas se conservan en la memoria persistente de la controladora. Para implementar la gestión de claves internas, siga estos pasos:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Cree una clave de seguridad interna, que implica definir un identificador y una frase de contraseña. El identificador es una frase que está asociada con la clave de seguridad, y se almacena en la controladora y en todas las unidades asociadas con la clave. La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. Para crear una clave interna, vaya a **MENU:Configuración[sistema > Gestión de claves de seguridad > Crear clave interna]**.

La clave de seguridad se almacena en una ubicación inaccesible de la controladora. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Gestión de claves externas

Las claves externas se mantienen en un servidor de gestión de claves individual mediante un protocolo de interoperabilidad de gestión de claves (KMIP). Para implementar la gestión de claves externas, siga estos pasos:


1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Complete y descargue una solicitud de firma de certificación (CSR) de cliente para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves. Vaya a **MENU:Configuración[certificados > Gestión de claves > completar CSR]**.
4. Cree y descargue un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado.

5. Asegúrese de que el certificado de cliente y una copia del certificado para el servidor de gestión de claves estén disponibles en el host local.
6. Cree una clave externa, que implica definir la dirección IP del servidor de gestión de claves y el número de puerto utilizado para comunicaciones KMIP. Durante este proceso, también debe cargar los archivos de certificado. Para crear una clave externa, vaya a **MENU:Settings[System > Security Key Management > Create External Key]**.

El sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Terminología de Drive Security

Conozca la forma en que los términos de Drive Security se aplican a su cabina de almacenamiento.

Duración	Descripción
Función Drive Security	Drive Security es una función de la cabina de almacenamiento que ofrece una capa adicional de seguridad con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security, se requiere una clave de seguridad para acceder a los datos. Cuando se retiran físicamente, las unidades de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta.
Unidades FDE	Las unidades de cifrado de disco completo (FDE) realizan el cifrado en la unidad de disco en el nivel de hardware. La unidad de disco duro contiene un chip ASIC que cifra los datos durante las escrituras y, a continuación, descifra los datos durante las lecturas.
Unidades FIPS	Las unidades con FIPS utilizan estándares de procesamiento de información federal (FIPS) 140-2 nivel 2. Son esencialmente unidades FDE que cumplen con las normas gubernamentales de los Estados Unidos para garantizar algoritmos y métodos de cifrado sólidos. Las unidades FIPS tienen normas de seguridad más rigurosas que las unidades FDE.
Cliente de gestión	Un sistema local (equipo, tablet, etc.) que incluye un explorador para acceder a System Manager.
Frase de contraseña	<p>La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. La misma frase de contraseña utilizada para cifrar la clave de seguridad debe incluirse cuando se importa la clave de seguridad como resultado de una migración de unidad o un cambio de cabezal. La frase de contraseña puede tener entre 8 y 32 caracteres.</p> <div>  <p>La frase de contraseña de Drive Security es independiente de la contraseña de administrador de la cabina de almacenamiento.</p> </div>

Duración	Descripción
Unidades compatibles con la función de seguridad	Las unidades compatibles con la función de seguridad pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS) que cifran datos durante la escritura y descifran datos durante la lectura. Estas unidades se consideran <i>Secure-capable</i> porque se pueden usar para obtener más seguridad mediante la función Drive Security. Si está habilitada la función Drive Security para los grupos de volúmenes y pools que se utilizan con estas unidades, las unidades pasan a tener habilitada la función de seguridad- <i>enabled</i> .
Unidades con la función de seguridad habilitada	Las unidades con la función de seguridad habilitada se usan con Drive Security. Cuando se habilita la función Drive Security y se aplica Drive Security a un pool o un grupo de volúmenes en unidades_ compatibles con la función de seguridad, las unidades pasan a ser seguras <i>habilitadas</i> . El acceso de lectura y escritura solo está disponible a través de una controladora que está configurada con la clave de seguridad correcta. Esta seguridad adicional evita el acceso no autorizado a los datos en una unidad que se quita físicamente de la cabina de almacenamiento.
Clave de seguridad	<p>Una clave de seguridad es una cadena de caracteres que se comparte entre las unidades habilitadas para seguridad y las controladoras en una cabina de almacenamiento. Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad. Si se elimina una unidad habilitada para seguridad de la cabina de almacenamiento, se bloquean los datos de esa unidad. Cuando se vuelve a instalar la unidad en otra cabina de almacenamiento, se busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad original. Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos:</p> <ul style="list-style-type: none"> • Gestión de claves internas: Crea y mantiene claves de seguridad en la memoria persistente de la controladora. • Gestión de claves externas: Crea y mantiene claves de seguridad en un servidor de gestión de claves externo.
Identificador de clave de seguridad	El identificador de clave de seguridad es una cadena asociada con la clave de seguridad durante su creación. El identificador se almacena en la controladora y en todas las unidades asociadas con la clave de seguridad.

Procedimientos

Cree una clave de seguridad interna

Para usar la función Drive Security, se puede crear una clave de seguridad interna que compartan las controladoras y las unidades compatibles con la función de seguridad de la cabina de almacenamiento. Las claves internas se conservan en la memoria persistente de la controladora.

Antes de empezar

- Se deben instalar unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
- Se debe habilitar la función Drive Security. De lo contrario, se abre el cuadro de diálogo no puede crearse una clave de seguridad durante esta tarea. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.



Si se instalan unidades FDE y FIPS en la cabina de almacenamiento, ambas compartirán la misma clave de seguridad.

Acerca de esta tarea

En esta tarea, se deben definir un identificador y una frase de contraseña para asociarlos con la clave de seguridad interna.



La frase de contraseña de Drive Security es independiente de la contraseña de administrador de la cabina de almacenamiento.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Gestión de claves de seguridad**, seleccione **Crear clave interna**.

Si aún no ha generado una clave de seguridad, se abre el cuadro de diálogo **Crear clave de seguridad**.

3. Introduzca información en los siguientes campos:

- **Definir un identificador de claves de seguridad:** Puede aceptar el valor predeterminado (Marca de tiempo y nombre de la cabina de almacenamiento, que genera el firmware de la controladora) o introducir el valor deseado. Puede introducir hasta 189 caracteres alfanuméricos sin espacios, puntuación ni símbolos.



Se generarán otros caracteres automáticamente, incorporados a ambos extremos de la cadena que introdujo. Los caracteres generados garantizan que el identificador sea único.

- **Definir una frase de contraseña/Volver a introducir la frase de contraseña** — Introduzca y confirme una frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
 - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
 - Un número (o varios).
 - Un carácter no alfanumérico, como !, *, @ (o varios).



Asegúrese de registrar lo introducido para usarlo en el futuro. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se deben conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

4. Haga clic en **Crear**.

La clave de seguridad se almacena en una ubicación inaccesible de la controladora. Además de la clave real, se descarga un archivo de claves cifrado del explorador.



La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

5. Anote el identificador de claves, la frase de la contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

Resultados

Ahora se pueden crear grupos de volúmenes o pools con la función de seguridad habilitada o puede habilitar la seguridad en los grupos de volúmenes y pools existentes.



Cada vez que se apagan y se vuelven a encender las unidades, todas las unidades con la función de seguridad habilitada cambian al estado Security Locked. En este estado, no se puede acceder a los datos hasta que la controladora aplica la clave de seguridad correcta durante la inicialización de la unidad. Si alguien quita físicamente la unidad bloqueada y la instala en otro sistema, el estado Security Locked evita el acceso no autorizado de los datos.

Después de terminar

Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Cree una clave de seguridad externa

Para usar la función Drive Security con un servidor de gestión de claves, se debe crear una clave externa que se compartirá con el servidor de gestión de claves y las unidades compatibles con la función de seguridad de la cabina de almacenamiento.

Antes de empezar

- Se deben instalar unidades compatibles con la función de seguridad en la cabina. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).



Si se instalan unidades FDE y FIPS en la cabina de almacenamiento, ambas compartirán la misma clave de seguridad.

- Se debe habilitar la función Drive Security. De lo contrario, se abre el cuadro de diálogo **no se puede crear la clave de seguridad** durante esta tarea. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
- Los certificados de cliente y de servidor están disponibles en el host local, por este motivo, el servidor de la cabina de almacenamiento y de gestión de claves pueden autenticarse entre sí. El certificado de cliente valida las controladoras, mientras que el certificado de servidor valida el servidor de gestión de claves.

Acerca de esta tarea

En esta tarea, se deben definir la dirección IP del servidor de gestión de claves y el número de puerto que utiliza y, luego, cargar los certificados para la gestión de claves externas.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Gestión de claves de seguridad**, seleccione **Crear clave externa**.



Si está configurada actualmente la gestión de claves internas, se muestra un cuadro de diálogo para solicitar la confirmación de que se desea cambiar a la gestión de claves externas.

Se abre el cuadro de diálogo **Crear clave de seguridad externa**.

3. En **conectar con el servidor de claves**, introduzca información en los siguientes campos:
 - **Dirección del servidor de administración de claves** — Introduzca el nombre de dominio completo o la dirección IP (IPv4 o IPv6) del servidor utilizado para la administración de claves.
 - **Número de puerto de administración de claves** — Introduzca el número de puerto utilizado para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El número de puerto más común que se usa para la comunicación del servidor de gestión de claves es 5696.
 - **Seleccionar certificado de cliente** — haga clic en el primer botón **examinar** para seleccionar el archivo de certificado para los controladores de la matriz de almacenamiento.
 - **Seleccione el certificado del servidor de administración de claves** — haga clic en el segundo botón **examinar** para seleccionar el archivo de certificado del servidor de administración de claves.

4. Haga clic en **Siguiente**.

5. En **Crear/hacer copia de seguridad de la clave**, introduzca información en el siguiente campo:

- **Definir una frase de contraseña/Volver a introducir la frase de contraseña** — Introduzca y confirme una frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
 - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
 - Un número (o varios).
 - Un carácter no alfanumérico, como !, *, @ (o varios).



Asegúrese de registrar lo introducido para usarlo en el futuro. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se debe conocer la frase de contraseña para desbloquear los datos de la unidad.

6. Haga clic en **Finalizar**.

El sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Luego, se almacena una copia de la clave de seguridad en el sistema local.



La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

7. Anote la frase de contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

En la página, se muestra el siguiente mensaje con enlaces adicionales para la gestión de claves externas.

Current key management method: External

8. Pruebe la conexión entre la cabina de almacenamiento y el servidor de gestión de claves. Para ello, seleccione **probar comunicación**.

Los resultados de la prueba se muestran en el cuadro de diálogo.

Resultados

Cuando se habilita la gestión de claves externas, se pueden crear grupos de volúmenes o pools con la función

de seguridad habilitada, o bien se puede habilitar la función de seguridad en los grupos de volúmenes y pools existentes.



Cada vez que se apagan y se vuelven a encender las unidades, todas las unidades con la función de seguridad habilitada cambian al estado Security Locked. En este estado, no se puede acceder a los datos hasta que la controladora aplica la clave de seguridad correcta durante la inicialización de la unidad. Si alguien quita físicamente la unidad bloqueada y la instala en otro sistema, el estado Security Locked evita el acceso no autorizado de los datos.

Después de terminar

- Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Cambiar clave de seguridad

Es posible reemplazar una clave de seguridad por una nueva en cualquier momento. Puede resultar necesario cambiar una clave de seguridad en aquellos casos en los que potencialmente se haya comprometido la seguridad en la empresa y en los que se desee garantizar que personal no autorizado no pueda acceder a los datos de las unidades.

Antes de empezar

Ya existe una clave de seguridad.

Acerca de esta tarea

En esta tarea, se describe cómo cambiar una clave de seguridad y reemplazarla por una nueva. Una vez completado este proceso, la clave anterior ya no es más válida.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Gestión de claves de seguridad**, seleccione **Cambiar clave**.

Se abre el cuadro de diálogo Cambiar clave de seguridad.

3. Introduzca información en los siguientes campos.

- **Definir un identificador de clave de seguridad** -- (sólo para claves de seguridad internas). Acepte el valor predeterminado (Marca de tiempo y nombre de la cabina de almacenamiento, que genera el firmware de la controladora) o introduzca un valor personalizado. Puede introducir hasta 189 caracteres alfanuméricos sin espacios, puntuación ni símbolos.



Se generan automáticamente caracteres adicionales y se agregan a ambos extremos de la cadena que introduce. Los caracteres generados ayudan a garantizar que el identificador sea único.

- **Definir una frase de contraseña/Volver a introducir la frase de contraseña** — en cada uno de estos campos, introduzca la frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
 - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
 - Un número (o varios).
 - Un carácter no alfanumérico, como !, *, @ (o varios).



Asegúrese de registrar las entradas para uso futuro.- Si necesita quitar de la cabina de almacenamiento una unidad con la función de seguridad habilitada, debe conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

4. Haga clic en **Cambiar**.

La clave de seguridad nueva sobrescribe la clave anterior, que ya no es válida.



La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

5. Anote el identificador de claves, la frase de la contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

Después de terminar

Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Alternar de gestión de claves internas a externas

Se puede modificar el método de gestión de Drive Security de un servidor de claves externo a un método interno utilizado por la cabina de almacenamiento. La clave de seguridad definida previamente para la gestión de claves externas luego se utiliza para la gestión de claves internas.

Antes de empezar

Se creó una clave externa.

Acerca de esta tarea

En esta tarea, se deshabilita la gestión de claves externas y se descarga una nueva copia de backup en el host local. La clave existente se sigue usando para Drive Security, pero se gestionará internamente en la cabina de almacenamiento.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Gestión de claves de seguridad**, seleccione **Desactivar administración de claves externa**.

Se abre el cuadro de diálogo **Deshabilitar administración de claves externa**.

3. En **definir una frase de contraseña/Volver a introducir la frase de contraseña**, introduzca y confirme una frase de contraseña para el backup de la clave. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
 - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
 - Un número (o varios).
 - Un carácter no alfanumérico, como !, *, @ (o varios).



Asegúrese de registrar las entradas para uso futuro. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se deben conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

4. Haga clic en **Desactivar**.

La clave de backup se descarga en el host local.

5. Anote el identificador de claves, la frase de la contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

Resultados

Drive Security ahora se gestiona internamente mediante la cabina de almacenamiento.

Después de terminar

- Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Editar configuración del servidor de gestión de claves

Si configuró la gestión de claves externas, es posible ver y editar los ajustes del servidor de gestión de claves en cualquier momento.

Antes de empezar

Debe configurarse la gestión de claves externas.

Pasos

1. Seleccione **MENU:Settings[Systems]**.
2. En **Gestión de claves de seguridad**, seleccione **Ver/editar configuración del servidor de administración de claves**.
3. Edite la información en los siguientes campos:
 - **Dirección del servidor de administración de claves** — Introduzca el nombre de dominio completo o la dirección IP (IPv4 o IPv6) del servidor utilizado para la administración de claves.
 - **Número de puerto KMIP** — Introduzca el número de puerto utilizado para las comunicaciones del Protocolo de interoperabilidad de gestión de claves (KMIP).
4. Haga clic en **Guardar**.

Realice un backup de la clave de seguridad

Después de crear o de cambiar una clave de seguridad, es posible crear una copia de backup del archivo de claves en caso de que el original se dañe.

Antes de empezar

- Ya existe una clave de seguridad.

Acerca de esta tarea

En esta tarea, se describe cómo realizar un backup de la clave de seguridad creada previamente. Durante este procedimiento, es posible crear una nueva frase de contraseña para el backup. No es necesario que esta frase de contraseña coincida con la utilizada cuando se creó o se modificó por última vez la clave original. La frase de contraseña se aplica solo al backup que se va a crear.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Gestión de claves de seguridad**, seleccione **clave de copia de seguridad**.

Se abre el cuadro de diálogo realizar backup de la clave de seguridad.

3. En los campos **define a pass phrase/Re-enter pass phrase**, introduzca y confirme una frase de contraseña para este backup.

El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:

- Una letra mayúscula (o varias)
- Un número (o varios).
- Un carácter no alfanumérico, como **!**, *****, **@** (o varios).



Asegúrese de registrar lo introducido para usarlo en el futuro. Necesita la frase de contraseña para acceder al backup de esta clave de seguridad.

4. Haga clic en **copia de seguridad**.

Se descarga una copia de seguridad de la clave de seguridad en el host local y, a continuación, se abre el cuadro de diálogo **Confirmar/registrar copia de seguridad de la clave**.



La ruta del archivo de claves de seguridad descargado puede depender de la ubicación de descarga predeterminada del explorador.

5. Registre la frase de contraseña en un lugar seguro y, a continuación, haga clic en **Cerrar**.

Después de terminar

Debe validar la clave de seguridad de backup.

Valide la clave de seguridad

Es posible validar la clave de seguridad para asegurarse de que no se haya dañado y verificar que tenga una frase de contraseña correcta.

Antes de empezar

Se creó una clave de seguridad.

Acerca de esta tarea

Esta tarea describe cómo validar la clave de seguridad que se creó anteriormente. Este es un paso importante para asegurarse de que el archivo de claves no esté dañado y que la frase de contraseña sea correcta. Esto permite acceder a datos de la unidad más adelante si se mueve una unidad con la función de seguridad habilitada de una cabina de almacenamiento a otra.

Pasos

1. Seleccione **MENU:Settings[System]**.
2. En **Gestión de claves de seguridad**, seleccione **Validar clave**.

Se abre el cuadro de diálogo **Validar clave de seguridad**.

3. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves (por ejemplo, `drivesecurity.slk`).
4. Introduzca la frase de contraseña asociada con la clave que seleccionó.

Al seleccionar un archivo de claves válido y una frase de contraseña, el botón **Validar** se vuelve disponible.

5. Haga clic en **Validar**.

Los resultados de la validación se muestran en el cuadro de diálogo.

6. Si los resultados muestran que la clave de seguridad se validó correctamente, haga clic en **Cerrar**. Si aparece un mensaje de error, siga las instrucciones sugeridas que se muestran en el cuadro de diálogo.

Desbloquee las unidades mediante una clave de seguridad

Si mueve unidades con la función de seguridad habilitada de una cabina de almacenamiento a otra, debe importar la clave de seguridad adecuada a la nueva cabina de almacenamiento. Al importar la clave, se desbloquean los datos de las unidades.

Antes de empezar

- La cabina de almacenamiento de destino (donde se moverán las unidades) ya debe tener una clave de seguridad configurada. Las unidades migradas se volverán a asignar una clave a la cabina de almacenamiento objetivo.
- Debe conocer la clave de seguridad asociada con las unidades que desea desbloquear.
- El archivo de claves de seguridad está disponible en el cliente de gestión (el sistema con un explorador que se utilizó para acceder a System Manager). Si mueve las unidades a una cabina de almacenamiento gestionada por otro sistema, debe mover el archivo de claves de seguridad a ese cliente de gestión.

Acerca de esta tarea

En esta tarea, se describe cómo desbloquear los datos de las unidades con la función de seguridad habilitada que se hayan eliminado de una cabina de almacenamiento y se hayan vuelto a instalar en otra. Una vez que la cabina detecta las unidades, aparece la condición "Needs Attention" junto con el estado "Security Key Needed" para estas unidades reubicadas. Para desbloquear los datos de la unidad, importe la clave de seguridad en la cabina de almacenamiento. Durante este proceso, se selecciona el archivo de claves de seguridad y se introduce la frase de contraseña para la clave.



La frase de contraseña no es la misma que la contraseña de administrador de la cabina de almacenamiento.

Si se instalan otras unidades con la función de seguridad habilitada en la nueva cabina de almacenamiento, estas podrían usar una clave de seguridad distinta de la que se está importando. Durante el proceso de importación, la clave de seguridad antigua se usa únicamente para desbloquear los datos de las unidades que se instalan. Cuando el proceso de desbloqueo se realiza correctamente, se vuelve a asignar una clave de seguridad de cabina de almacenamiento de destino a las unidades recién instaladas.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Desbloquear unidades seguras**.

Se abre el cuadro de diálogo Desbloquear unidades seguras. Todas las unidades que requieren una clave de seguridad se muestran en la tabla.

3. **Opcional:** pase el ratón sobre un número de unidad para ver la ubicación de la unidad (número de bandeja y número de bahía).

4. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves de seguridad correspondiente a la unidad que desea desbloquear.

El archivo de claves seleccionado aparece en el cuadro de diálogo.

5. Introduzca la frase de contraseña asociada con este archivo de claves.

Los caracteres introducidos están enmascarados.

6. Haga clic en **Desbloquear**.

Si la operación de desbloqueo se realiza correctamente, en el cuadro de diálogo se muestra un mensaje que indica que se desbloquearon las unidades seguras asociadas.

Resultados

Cuando todas las unidades se bloquean y después se desbloquean, se reinicia cada controladora de la cabina de almacenamiento. Sin embargo, si ya existen algunas unidades desbloqueadas en la cabina de almacenamiento de destino, las controladoras no se reinician.

Preguntas frecuentes

¿Qué debo saber antes de crear una clave de seguridad?

Las controladoras y unidades con seguridad habilitada comparten una clave de seguridad dentro de una cabina de almacenamiento. Si se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento, la clave de seguridad protege los datos de un acceso no autorizado.

Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos:

- Gestión de claves internas en la memoria persistente de la controladora.
- Gestión de claves externas en un servidor de gestión de claves externo.

Antes de crear una clave de seguridad interna, debe hacer lo siguiente:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.

Luego, podrá crear una clave de seguridad interna, lo que implica definir un identificador y una frase de contraseña. El identificador es una frase que está asociada con la clave de seguridad, y se almacena en la controladora y en todas las unidades asociadas con la clave. La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. Una vez que haya terminado, la clave de seguridad se almacena en una ubicación no accesible de la controladora. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Antes de crear una clave de seguridad externa, debe hacer lo siguiente:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información

federal (FIPS).

2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Complete y descargue una solicitud de firma de certificación (CSR) de cliente para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves. Vaya a **MENU:Configuración[certificados > Gestión de claves > completar CSR]**.
4. Cree y descargue un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado.
5. Asegúrese de que el certificado de cliente y una copia del certificado para el servidor de gestión de claves estén disponibles en el host local.

Luego, podrá crear una clave externa, lo que implica definir la dirección IP del servidor de gestión de claves y el número de puerto para las comunicaciones KMIP. Durante este proceso, también debe cargar los archivos de certificado. Una vez que haya terminado, el sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

¿Por qué debo definir una frase de contraseña?

La frase de contraseña se utiliza para cifrar y descifrar el archivo de claves de seguridad almacenado en el cliente de gestión local. Sin la frase de contraseña, la clave de seguridad no se puede descifrar y utilizar para desbloquear datos de una unidad con la función de seguridad habilitada, si se la reinstala en otra cabina de almacenamiento.

¿Por qué es importante registrar la información de claves de seguridad?

Si pierde la información de la clave de seguridad y no cuenta con un backup, podría perder los datos al reubicar las unidades con la función de seguridad habilitada o actualizar una controladora. La clave de seguridad es necesaria para desbloquear los datos en las unidades.

Asegúrese de registrar el identificador de la clave de seguridad, la frase de contraseña asociada y la ubicación en el host local en donde se guardó el archivo de claves de seguridad.

¿Qué debo saber antes de realizar un backup de una clave de seguridad?

Si la clave de seguridad original se daña y no existe un backup, se perderá el acceso a los datos de las unidades al migrarlas de una cabina de almacenamiento a otra.

Antes de realizar el backup de una clave de seguridad, tenga en cuenta las siguientes directrices:

- Asegúrese de conocer el identificador de claves de seguridad y la frase de contraseña del archivo de claves original.



Solo las claves internas usan identificadores. Cuando se crea el identificador, se crean caracteres adicionales que se anexan automáticamente a ambos extremos de la cadena del identificador. Los caracteres generados garantizan que el identificador sea único.

- Es posible crear una frase de contraseña nueva para el backup. No es necesario que esta frase de contraseña coincida con la utilizada cuando se creó o se modificó por última vez la clave original. La frase

de contraseña solo se aplica al backup que se crea.



La frase de contraseña para Drive Security no debería confundirse con la contraseña del administrador de la cabina de almacenamiento. La frase de contraseña para Drive Security protege los backups de una clave de seguridad. La contraseña del administrador protege toda la cabina de almacenamiento de un acceso no autorizado.

- El archivo de claves de seguridad de backup se descarga en el cliente de gestión. La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador. Asegúrese de registrar dónde se almacena la información de la clave de seguridad.

¿Qué debo saber antes de desbloquear unidades seguras?

Para desbloquear los datos de una unidad compatible con la función de seguridad habilitada que se migra a una cabina de almacenamiento nueva, se debe importar la clave de seguridad.

Antes de desbloquear unidades con la función de seguridad habilitada, recuerde las siguientes directrices:

- La cabina de almacenamiento de destino (donde se moverán las unidades) ya debe tener una clave de seguridad. Las unidades migradas se volverán a asignar una clave a la cabina de almacenamiento objetivo.
- Para las unidades que se van a migrar, se deben conocer el identificador de la clave de seguridad y la frase de contraseña que corresponden al archivo de claves de seguridad.
- El archivo de claves de seguridad está disponible en el cliente de gestión (el sistema con un explorador que se utilizó para acceder a System Manager).
- Si va a restablecer una unidad NVMe bloqueada, debe introducir el identificador de seguridad de la unidad. Para ubicarlo, retire físicamente la unidad y busque la cadena de PSID (máximo de 32 caracteres) en la etiqueta de la unidad. Asegúrese de reinstalar la unidad antes de iniciar la operación.

¿Qué es la accesibilidad de lectura/escritura?

La ventana Configuración de la unidad incluye información acerca de los atributos de seguridad de la unidad. "Read/Write Accessible" es uno de los atributos que se muestran si se bloquearon los datos de una unidad.

Para ver los atributos de Drive Security, vaya a la página hardware. Seleccione una unidad, haga clic en **Ver configuración** y, a continuación, haga clic en **Mostrar más valores**. En la parte inferior de la página, el valor del atributo Accesibilidad de lectura/escritura será **Sí** cuando la unidad esté desbloqueada. El valor del atributo Accesibilidad de lectura/escritura es **no, clave de seguridad no válida** cuando la unidad está bloqueada. Si desea desbloquear una unidad segura, importe una clave de seguridad (vaya a menú:Configuración[sistema > Desbloquear unidades seguras]).

¿Qué debo saber acerca de la validación de la clave de seguridad?

Después de crear una clave de seguridad, se debe validar el archivo de claves para garantizar que no esté dañado.

Si la validación falla, haga lo siguiente:

- Si el identificador de claves de seguridad no coincide con el identificador de la controladora, busque el

archivo de claves de seguridad correcto y vuelva a intentar hacer la validación.

- Si la controladora no puede descifrar la clave de seguridad para la validación, es posible que haya introducido incorrectamente la frase de contraseña. Haga doble clic en la frase de contraseña, vuelva a introducirla si fuera necesario y vuelva a intentar hacer la validación. Si vuelve a aparecer el mensaje de error, seleccione un backup del archivo de claves (si estuviera disponible) y vuelva a intentar hacer la validación.
- Si aún no puede validar la clave de seguridad, es posible que el archivo original esté dañado. Cree un backup nuevo de la clave y valide esa copia.

¿Cuál es la diferencia entre la gestión de claves de seguridad interna y de claves de seguridad externa?

Cuando se implementa la función Drive Security, es posible utilizar una clave de seguridad interna o una clave de seguridad externa para bloquear los datos cuando se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento.

Una clave de seguridad es una cadena de caracteres, que se comparte entre las unidades y controladoras con la función de seguridad habilitada en una cabina de almacenamiento. Las claves internas se conservan en la memoria persistente de la controladora. Las claves externas se mantienen en un servidor de gestión de claves individual mediante un protocolo de interoperabilidad de gestión de claves (KMIP).

Access Management

Conceptos

Cómo funciona Access Management

Access Management es un método para establecer la autenticación de usuario en SANtricity System Manager.

La configuración y la autenticación de usuarios de Access Management funciona de la siguiente manera:

1. Un administrador inicia sesión en System Manager con un perfil de usuario que incluye permisos de administración de seguridad.



La primera vez que se inicia sesión, el nombre de usuario `admin` se muestra automáticamente y no se puede cambiar. La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. El administrador navega hasta Access Management en la interfaz de usuario. La cabina de almacenamiento está preconfigurada para utilizar roles de usuario local, que son una implementación de capacidades RBAC (control de acceso basado en roles).
3. El administrador configura uno o varios de los siguientes métodos de autenticación:
 - **Roles de usuario local** — la autenticación se gestiona a través de capacidades RBAC aplicadas en la cabina de almacenamiento. Los roles de usuario local incluyen perfiles de usuario predefinidos con permisos de acceso específicos. Los administradores pueden usar estos roles de usuario local como el único método de autenticación o usarlos en combinación con un servicio de directorio. No hace falta configurar nada más allá de las contraseñas de los usuarios.
 - **Servicios de directorio** — la autenticación se administra a través de un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorio, como Active Directory de Microsoft. Un

administrador se conecta con el servidor LDAP y luego asigna los usuarios LDAP a los roles de usuario local integrados en la cabina de almacenamiento.

- **SAML** — la autenticación se gestiona a través de un proveedor de identidades (IDP) utilizando el lenguaje de marcado de aserción de seguridad (SAML) 2.0. Un administrador establece comunicación entre el sistema IDP y la cabina de almacenamiento, y luego asigna los usuarios IDP a los roles de usuario local integrados en la cabina de almacenamiento.

4. El administrador ofrece credenciales de inicio de sesión en System Manager para los usuarios.
5. Los usuarios inician sesión en el sistema con sus credenciales.



Si la autenticación se gestiona con SAML y un SSO (inicio de sesión único), el sistema puede omitir el diálogo de inicio de sesión de System Manager.

Durante el inicio de sesión, el sistema realiza las siguientes tareas en segundo plano:

- Autentica el nombre de usuario y la contraseña en relación con la cuenta de usuario.
- Determina los permisos del usuario según los roles asignados.
- Ofrece acceso al usuario a las tareas en la interfaz de usuario.
- Muestra el nombre de usuario en la esquina superior derecha de la interfaz.

Tareas disponibles en System Manager

El acceso a las tareas depende de los roles asignados a un usuario, entre los cuales se encuentran los siguientes:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento (por ejemplo, volúmenes y pools de discos), pero sin acceso a la configuración de seguridad.
- **Administración de seguridad** — acceso a la configuración de seguridad en Access Management, administración de certificados, administración de registros de auditoría y la capacidad de activar o desactivar la interfaz de administración heredada (Symbol).
- **Support admin** — acceso a todos los recursos de hardware en la cabina de almacenamiento, datos de fallos, eventos MEL y actualizaciones del firmware de la controladora. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Una tarea no disponible está atenuada o no aparece en la interfaz de usuario. Por ejemplo, un usuario con el rol de supervisión puede ver toda la información sobre los volúmenes, pero no puede acceder a funciones para modificarlos. Las pestañas para funciones como **Servicios de copia** y **Agregar a carga de trabajo** estarán atenuadas; sólo **Ver/Editar configuración** está disponible.

Limitaciones en Unified Manager de SANtricity y Storage Manager de SANtricity

Si se configura SAML para una cabina de almacenamiento, los usuarios no pueden detectar ni gestionar el almacenamiento de esa cabina desde las interfaces de SANtricity Unified Manager o SANtricity Storage Manager.

Cuando se configuran los roles de usuario local y los servicios de directorio, los usuarios deben introducir credenciales para poder realizar cualquiera de las siguientes funciones:

- Cambiar el nombre de la cabina de almacenamiento

- Actualizar el firmware de la controladora
- Cargar una configuración de la cabina de almacenamiento
- Ejecutar un script
- Intentar realizar una operación activa cuando se agotó el tiempo de espera de una sesión no utilizada

Terminología de Access Management

Conozca la forma en que los términos de Access Management se aplican a su cabina de almacenamiento.

Duración	Descripción
Active Directory	Active Directory (AD) es un servicio de directorio de Microsoft en el que se utiliza LDAP para redes de dominio de Windows.
Vinculación	Las operaciones de vinculación se usan para autenticar clientes en el servidor de directorio. Por lo general, la vinculación requiere credenciales de cuenta y contraseña, pero algunos servidores aceptan operaciones de vinculación anónimas.
APROX	Una entidad de certificación (CA) es una entidad de confianza que emite documentos electrónicos, denominados certificados digitales, para la seguridad de Internet. Estos certificados identifican a los propietarios de sitios web y, de esta manera, permiten conexiones seguras entre clientes y servidores.
Certificado	Un certificado identifica al propietario de un sitio con el fin de brindar seguridad, para evitar que atacantes se hagan pasar por los propietarios del sitio. El certificado tiene información acerca del propietario del sitio y la identidad de la entidad de confianza que certifica (firma) esta información.
IDP	Un proveedor de identidades (IDP) es un sistema externo que se usa para solicitar credenciales a un usuario y para determinar si el usuario se autentica correctamente. El IDP se puede configurar para ofrecer autenticación multifactor y para usar cualquier base de datos de usuario, como Active Directory. El equipo de seguridad es responsable de mantener el IDP.
LDAP	El protocolo ligero de acceso a directorios (LDAP) es un protocolo de aplicación para acceder a servicios distribuidos de información de directorio y mantenerlos. Este protocolo permite que varias aplicaciones y servicios se conecten con el servidor LDAP para validar usuarios.
RBAC	El control de acceso basado en funciones (RBAC) es un método para regular el acceso a los recursos informáticos o de red en función de las funciones de los usuarios individuales. Los controles de RBAC se aplican en la cabina de almacenamiento y se componen de roles predefinidos.

Duración	Descripción
SAML	El lenguaje de marcado de aserción de seguridad (SAML) es un estándar basado en XML para fines de autenticación y autorización entre dos entidades. SAML permite utilizar la autenticación multifactor, en la cual los usuarios deben introducir dos o más elementos para validar su identidad (por ejemplo, una contraseña y una huella digital). La función de SAML integrada de la cabina de almacenamiento es compatible con SAML2.0 para autenticación, autorización y confirmación de identidades.
SP	Un proveedor de servicios (SP) es un sistema que controla la autenticación y el acceso de usuario. Cuando se configura Access Management con SAML, la cabina de almacenamiento actúa como proveedor de servicios, ya que solicita la autenticación del proveedor de identidades.
SSO	El inicio de sesión único (SSO) es un servicio de autenticación que permite el uso de un conjunto de credenciales de inicio de sesión para acceder a varias aplicaciones.

Permisos para roles asignados

Las capacidades de RBAC (control de acceso basado en roles) presentes en la cabina de almacenamiento incluyen perfiles de usuario predefinidos con uno o varios roles asignados. Cada rol incluye permisos para acceder a tareas en SANtricity System Manager.

Se puede acceder a los perfiles de usuario y a los roles asignados desde **menú:Configuración[Administración de acceso > roles de usuario local]** en la interfaz de usuario de cualquiera de los Administrador del sistema.

Los roles permiten que los usuarios accedan a tareas de la siguiente manera:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento (por ejemplo, volúmenes y pools de discos), pero sin acceso a la configuración de seguridad.
- **Administración de seguridad** — acceso a la configuración de seguridad en Access Management, administración de certificados, administración de registros de auditoría y la capacidad de activar o desactivar la interfaz de administración heredada (Symbol).
- **Support admin** — acceso a todos los recursos de hardware en la cabina de almacenamiento, datos de fallos, eventos MEL y actualizaciones del firmware de la controladora. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Si un usuario no tiene permisos para determinada tarea, la tarea aparece atenuada o directamente no aparece en la interfaz de usuario.

Access Management con roles de usuario local

Para Access Management, los administradores pueden usar las capacidades RBAC (control de acceso basado en roles) aplicadas en la cabina de almacenamiento. Estas

capacidades se denominan "roles de usuario local".

Flujo de trabajo de configuración

Los roles de usuario local están preconfigurados para la cabina de almacenamiento. Para usar roles de usuario local con fines de autenticación, los administradores pueden hacer lo siguiente:

1. Un administrador inicia sesión en SANtricity System Manager con un perfil de usuario que incluye permisos de administración de seguridad.



La admin el usuario tiene acceso completo a todas las funciones del sistema.

2. Un administrador revisa los perfiles de usuario, que están predefinidos y no pueden modificarse.
3. **Opcional:** el administrador asigna nuevas contraseñas para cada perfil de usuario.
4. Los usuarios inician sesión en el sistema con las credenciales asignadas.

Gestión

Al utilizar solamente los roles de usuario local para la autenticación, los administradores pueden realizar las siguientes tareas de gestión:

- Cambiar contraseñas.
- Configurar la longitud mínima de las contraseñas.
- Permitir que los usuarios inicien sesión sin contraseñas.

Access Management con servicios de directorio

Para Access Management, los administradores puede usar un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorios, como Active Directory de Microsoft.

Flujo de trabajo de configuración

Si se utilizan un servidor LDAP y un servicio de directorio en la red, la configuración opera de la siguiente manera:

1. Un administrador inicia sesión en SANtricity System Manager con un perfil de usuario que incluye permisos de administración de seguridad.



La admin el usuario tiene acceso completo a todas las funciones del sistema.

2. El administrador introduce los ajustes de configuración del servidor LDAP. Entre ellas se encuentran el nombre de dominio, la URL y la información de la cuenta vinculada.
3. Si el servidor LDAP utiliza un protocolo seguro (LDAPS), el administrador carga una cadena de certificados de Certificate Authority (CA) para la autenticación entre el servidor LDAP y la cabina de almacenamiento.
4. Después de establecer la conexión del servidor, el administrador asigna los grupos de usuarios a los roles de la cabina de almacenamiento. Estos roles están predefinidos y no pueden modificarse.
5. El administrador prueba la conexión entre el servidor LDAP y la cabina de almacenamiento.

6. Los usuarios inician sesión en el sistema con las credenciales de LDAP/servicios de directorio asignadas.

Gestión

Al utilizar los servicios de directorio para la autenticación, los administradores pueden realizar las siguientes tareas de gestión:

- Añadir servidor de directorio.
- Editar la configuración del servidor de directorio.
- Asignar usuarios LDAP a roles de usuario local.
- Quitar un servidor de directorio.

Access Management con SAML

Para Access Management, los administradores pueden usar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) 2.0 que están integradas en la cabina.

Flujo de trabajo de configuración

La configuración de SAML funciona de la siguiente manera:

1. Un administrador inicia sesión en System Manager con un perfil de usuario que incluye permisos de administración de seguridad.



La admin El usuario tiene acceso completo a todas las funciones en System Manager.

2. El administrador se dirige a la ficha **SAML** de Access Management.
3. Un administrador configura las comunicaciones con el proveedor de identidades (IDP). Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. Para configurar las comunicaciones con la cabina de almacenamiento, el administrador descarga el archivo de metadatos de IDP desde el sistema IDP y luego usa System Manager para cargarlo a la cabina de almacenamiento.
4. Un administrador establece una relación de confianza entre el proveedor de servicios y el IDP. Un proveedor de servicios controla la autorización de usuarios; en este caso, la controladora en la cabina de almacenamiento actúa como proveedor de servicios. Para configurar las comunicaciones, el administrador usa System Manager para exportar el archivo de metadatos del proveedor de servicios en cada controladora. Desde el sistema IDP, el administrador importa estos archivos de metadatos al IDP.



Los administradores también deben asegurarse de que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.

5. El administrador asigna los roles de la cabina de almacenamiento a los atributos de usuario definidos en el IDP. Para hacerlo, el administrador usa System Manager y crea las asignaciones.
6. El administrador prueba el inicio de sesión de SSO en la URL del IDP. Esta prueba garantiza que la cabina de almacenamiento y el IDP puedan comunicarse.



Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

7. En System Manager, el administrador del sistema habilita SAML para la cabina de almacenamiento.
8. Los usuarios inician sesión en el sistema con sus credenciales de SSO.

Gestión

Cuando se usa SAML con fines de autenticación, los administradores pueden realizar las siguientes tareas de administración:

- Modifique o cree nuevas asignaciones de roles
- Exporte los archivos del proveedor de servicios

Restricciones de acceso

Cuando se habilita SAML, los usuarios no pueden detectar ni gestionar el almacenamiento de esa cabina desde las interfaces de SANtricity Unified Manager o SANtricity Storage Manager.

Además, los siguientes clientes no pueden obtener acceso a los recursos y los servicios de la cabina de almacenamiento:

- Enterprise Management Window (EMW)
- Interfaz de línea de comandos (CLI)
- Clientes de kits de desarrollo de software (SDK)
- Clientes en banda
- Clientes HTTP de la API de REST de autenticación básica
- Inicio de sesión mediante extremo estándar de la API de REST

Procedimientos

Ver los roles de usuario local

Desde la pestaña roles de usuario local, es posible ver las asignaciones de los perfiles de usuario a los roles predeterminados. Estas asignaciones forman parte de los controles de acceso basados en roles (RBAC) aplicados en la cabina de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

Los perfiles de usuario y las asignaciones no pueden cambiarse. Solo las contraseñas pueden modificarse.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.

2. Seleccione la ficha **roles de usuario local**.

Los perfiles de usuario se muestran en la tabla:

- **Administrador raíz** (admin) — Super administrador que tiene acceso a todas las funciones del sistema. Este perfil de usuario incluye todos los roles.
- **Administrador de almacenamiento** (almacenamiento) — el administrador responsable de todo el aprovisionamiento de almacenamiento. Este perfil de usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y Supervisión.
- **Administración de seguridad** (seguridad): El usuario responsable de la configuración de seguridad, incluidas la administración de acceso, la administración de certificados y las funciones de unidad con seguridad habilitada. Este perfil de usuario incluye los siguientes roles: Administrador de seguridad y Supervisión.
- **Support admin** (asistencia técnica) — el usuario responsable de recursos de hardware, datos de fallos y actualizaciones de firmware. Este perfil de usuario incluye los siguientes roles: Support Admin y Supervisión.
- **Monitor** (monitor) — un usuario con acceso de sólo lectura al sistema. Este perfil de usuario incluye únicamente el rol Supervisión.

Cambiar contraseñas

Es posible cambiar las contraseñas de usuario de cada perfil de usuario desde Access Management.

Antes de empezar

- Inició sesión como administrador local, lo que incluye permisos de administrador raíz.
- Debe conocer la contraseña de administrador local.

Acerca de esta tarea

Tenga en cuenta estas directrices al elegir una contraseña:

- Todas las contraseñas de usuarios locales nuevas deben alcanzar o superar la configuración de longitud mínima actual de la contraseña (en Ver/editar configuración).
- Las contraseñas distinguen mayúsculas de minúsculas.
- Los espacios al final de la contraseña no se eliminan, si se los utiliza. Procure incluir espacios si se incluyeron en la contraseña.
- Para mayor seguridad, use al menos 15 caracteres alfanuméricos y cambie la contraseña con frecuencia.



Cuando se cambia la contraseña en System Manager también se modifica en la interfaz de línea de comandos (CLI). Además, los cambios de contraseña provocan el cierre de la sesión activa del usuario.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione un usuario de la tabla.

Se habilita el botón Cambiar contraseña.

4. Seleccione **Cambiar contraseña**.

Se abre el cuadro de diálogo Cambiar contraseña.

5. Si no se estableció una longitud de contraseña mínima para las contraseñas de usuario local, se puede marcar la casilla para solicitar que el usuario seleccionado introduzca una contraseña para acceder a la cabina de almacenamiento y, a continuación, se puede escribir la contraseña nueva para el usuario seleccionado.
6. Introduzca su contraseña de administrador local y, a continuación, haga clic en **Cambiar**.

Resultados

Si el usuario está conectado, el cambio de contraseña provocará el cierre de la sesión activa del usuario.

Cambie la configuración de contraseña de usuario local

Es posible configurar la longitud mínima requerida para todas las contraseñas de usuario locales nuevas o actualizadas de la cabina de almacenamiento. También es posible permitir a los usuarios locales acceder a la cabina de almacenamiento sin introducir una contraseña.

Antes de empezar

- Inició sesión como administrador local, lo que incluye permisos de administrador raíz.

Acerca de esta tarea

Recuerde estas directrices cuando configure la longitud mínima para las contraseñas de usuario local:

- Los cambios en la configuración no afectan a las contraseñas existentes de usuarios locales.
- La configuración de la longitud mínima requerida para las contraseñas de usuario local debe tener entre 0 y 30 caracteres.
- Todas las contraseñas de usuario local nuevas deben alcanzar o superar la configuración de longitud mínima actual.
- No configure una longitud mínima para la contraseña si no desea que usuarios locales accedan a la cabina de almacenamiento sin introducir una contraseña.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione el botón **Ver/editar configuración**.

Se abre el cuadro de diálogo **Configuración de contraseña de usuario local**.

4. Debe realizar una de las siguientes acciones:
 - Para permitir a los usuarios locales acceder a la cabina de almacenamiento *sin* introducir una contraseña, desactive la casilla de comprobación "require all local user passwords to be at least".
 - Para configurar una longitud mínima de contraseña para todas las contraseñas de usuarios locales, active la casilla de comprobación "require all local user passwords to be at least" y luego use el cuadro de desplazamiento para configurar la longitud mínima requerida para todas las contraseñas de usuarios locales.

Todas las contraseñas de usuario local nuevas deben alcanzar o superar la configuración actual.

5. Haga clic en **Guardar**.

Añadir servidor de directorio

Para configurar la autenticación de Access Management, se pueden establecer comunicaciones entre la cabina de almacenamiento y un servidor LDAP, y luego asignar los grupos de usuarios LDAP a los roles predefinidos de la cabina.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.
- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

Acerca de esta tarea

La adición de un servidor de directorio es un proceso que consta de dos pasos. Primero, se debe introducir la URL y el nombre de dominio. Si el servidor utiliza un protocolo seguro, se debe cargar además un certificado de CA para autenticación, si no está firmado por una entidad de firma estándar. Si se poseen credenciales de una cuenta de enlace, también es posible introducir el nombre de cuenta de usuario y la contraseña. Luego, se deben asignar los grupos de usuarios del servidor LDAP a los roles predefinidos de la cabina de almacenamiento.



Durante el procedimiento para añadir un servidor LDAP, se deshabilitará la interfaz de gestión heredada. La interfaz de gestión heredada (Symbol) es un método de comunicación entre la cabina de almacenamiento y el cliente de gestión. Cuando se encuentra deshabilitada, la cabina de almacenamiento y el cliente de gestión utilizan un método de comunicación más seguro (API DE REST por https).

Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. En la ficha **Servicios de directorio**, seleccione **Agregar servidor de directorio**.


Se abre el cuadro de diálogo Añadir servidor de directorio.

3. En la ficha **Configuración del servidor**, introduzca las credenciales del servidor LDAP.

Detalles del campo

Ajuste	Descripción
Ajustes de configuración	Dominios
Introduzca el nombre de dominio del servidor LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (<i>username@domain</i>) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
Introduzca la URL para acceder al servidor LDAP con el formato de <code>ldap[s]://host:*port*</code> .	Cargar certificado (opcional)

Ajuste	Descripción
<div data-bbox="245 363 302 415" data-label="Image"> </div> <p data-bbox="362 170 480 611">Este campo aparece solo si se especifica a un protocolo LDAPS en el campo URL del servidor arriba.</p> <p data-bbox="212 659 509 961">Haga clic en examinar y seleccione un certificado de CA para cargar. Este es el certificado o la cadena de certificados de confianza utilizado para autenticar el servidor LDAP.</p>	<p data-bbox="529 159 846 191">Enlazar cuenta (opcional)</p>
<p data-bbox="212 1014 509 1560">Introduzca una cuenta de usuario de solo lectura para realizar consultas de búsqueda en el servidor LDAP y para buscar dentro de los grupos. Introduzca el nombre de cuenta con formato tipo LDAP. Por ejemplo, si el usuario de enlace se denomina "bindacct", puede introducir un valor como el siguiente: "CN=bindacct,CN=Users,DC=cpoc,DC=local".</p>	<p data-bbox="529 1014 899 1045">Enlazar contraseña (opcional)</p>

Ajuste		Descripción
 <p>Este campo aparece cuando introduce una cuenta de enlace arriba.</p> <p>Introduzca la contraseña de la cuenta de enlace.</p>		Probar conexión del servidor antes de añadir
	<p>Seleccione esta casilla de comprobación si desea asegurarse de que la cabina de almacenamiento pueda comunicarse con la configuración de servidor LDAP que introdujo. La prueba se produce después de hacer clic en Agregar en la parte inferior del cuadro de diálogo. Si esta casilla de comprobación está seleccionada y la prueba falla, no se añadirá la configuración. Debe resolver el error o anular la selección de la casilla de comprobación para omitir la comprobación y añadir la configuración.</p>	Ajustes de privilegios
DN base de búsqueda		Introduzca el contexto de LDAP para buscar usuarios, generalmente con el formato de CN=Users, DC=copc, DC=local.
Atributo de nombre de usuario		Introduzca el atributo vinculado al ID de usuario para los fines de autenticación. Por ejemplo: sAMAccountName.

Ajuste	Descripción
Atributos de grupo	Introduzca una lista de atributos de grupo en el usuario, que se utilizará para la asignación de grupos a roles. Por ejemplo: <code>memberOf</code> , <code>managedObjects</code> .

- Haga clic en la ficha **asignación de roles**.
- Asigne grupos LDAP a los roles predefinidos. Un grupo puede tener varios roles asignados.

Detalles del campo

Ajuste	Descripción
Asignaciones	DN de grupo
Especifique el nombre distintivo (DN) del grupo correspondiente al grupo de usuarios LDAP que se asignará.	Funciones



El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

- Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
- Cuando termine de asignar, haga clic en **Agregar**.

El sistema realiza una validación y se asegura de que la cabina de almacenamiento y el servidor LDAP pueden comunicarse. Si aparece un mensaje de error, compruebe las credenciales que introdujo en el cuadro de diálogo y vuelva a introducir la información, de ser necesario.

Editar ajustes y asignaciones de roles del servidor de directorios

Si anteriormente configuró un servidor de directorio en Access Management, es posible cambiar sus ajustes en cualquier momento. Entre estos ajustes se encuentran la información de conexión del servidor y las asignaciones de grupos a roles.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe definirse un servidor de directorio.

Pasos

- Seleccione **MENU:Settings[Access Management]**.
- Seleccione la ficha **Servicios de directorio**.

3. Si se define más de un servidor, seleccione el servidor que desea editar en la tabla.
4. Seleccione **Ver/editar configuración**.

Se abre el cuadro de diálogo **Configuración del servidor de directorio**.

5. En la ficha **Configuración del servidor**, cambie la configuración deseada.

Ajuste	Descripción
Ajustes de configuración	Dominios
Los nombres de dominio de los servidores LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (<i>username@domain</i>) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
La URL para acceder al servidor LDAP con el formato de <code>ldap[s]://host:*port*</code> .	Enlazar cuenta (opcional)
La cuenta de usuario de solo lectura para realizar consultas en el servidor LDAP y buscar dentro de grupo.	Enlazar contraseña (opcional)
La contraseña de la cuenta vinculada. (Este campo se muestra cuando se introduce una cuenta vinculada.)	Probar conexión del servidor antes de guardar

Ajuste	Descripción
Comprueba que la cabina de almacenamiento pueda comunicarse con la configuración del servidor LDAP. La prueba se produce después de hacer clic en Guardar en la parte inferior del cuadro de diálogo. Si se selecciona esta casilla de comprobación y la prueba falla, no se modifica la configuración. Debe resolver el error o cancelar la selección de la casilla de comprobación para omitir la prueba y volver a editar la configuración.	Configuración de privilegios
DN base de búsqueda	
Atributo de nombre de usuario	
Atributos de grupo	

6. En la ficha **asignación de roles**, cambie la asignación deseada.

Ajuste	Descripción
Asignaciones	DN de grupo
El nombre de dominio para asignar el grupo de usuarios LDAP.	Funciones



El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

7. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.

8. Haga clic en **Guardar**.

Resultados

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Quitar un servidor de directorio

Para interrumpir la conexión entre un servidor de directorio y la cabina de almacenamiento, es posible eliminar la información del servidor de la página Access Management. Se recomienda ejecutar esta tarea si se configuró un servidor nuevo y se desea eliminar el anterior.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. Seleccione la ficha **Servicios de directorio**.
3. Seleccione el servidor de directorio que desea eliminar de la lista.
4. Haga clic en **Quitar**.

Se abrirá el cuadro de diálogo **Quitar servidor de directorio**.

5. Tipo `remove` En el campo y, a continuación, haga clic en **Quitar**.

Se eliminará la configuración del servidor de directorio, la configuración de privilegios y las asignaciones de roles. Los usuarios ya no podrán iniciar sesión con las credenciales de este servidor.

Configure SAML

Para configurar la autenticación de Access Management, puede usar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) que están integradas en la cabina de almacenamiento. Esta configuración establece una conexión entre un proveedor de identidades y el proveedor de almacenamiento.

Acerca de esta tarea

Un proveedor de identidades (IDP) es un sistema externo que se usa para solicitar credenciales a un usuario y para determinar si el usuario se autentica correctamente. El IDP se puede configurar para ofrecer autenticación multifactor y para usar cualquier base de datos de usuario, como Active Directory. El equipo de seguridad es responsable de mantener el IDP. Un proveedor de servicios (SP) es un sistema que controla la autenticación y el acceso de usuario. Cuando se configura Access Management con SAML, la cabina de almacenamiento actúa como proveedor de servicios, ya que solicita la autenticación del proveedor de identidades. Para establecer una conexión entre el IDP y la cabina de almacenamiento, se deben compartir archivos de metadatos entre estas dos entidades. A continuación, se deben asignar las entidades de usuario

de IDP con los roles de la cabina de almacenamiento. Y, finalmente, se debe probar la conexión y los inicios de sesión SSO antes de habilitar SAML.



SAML y Directory Services. Si SAML se habilita cuando Directory Services está configurado como método de autenticación, SAML sustituye a Directory Services en System Manager. Si se deshabilita SAML posteriormente, la configuración de Directory Services se establece en los valores anteriores.



Edición y desactivación. una vez que SAML está habilitado, *no puede* desactivarlo a través de la interfaz de usuario, ni puede editar la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

La configuración de la autenticación SAML es un procedimiento de varios pasos.

Paso 1: Cargue el archivo de metadatos de IDP

Para brindar información de conexión de IDP a la cabina de almacenamiento, se deben importar los metadatos de IDP en System Manager.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Un administrador de IDP configuró un sistema IDP.
- Un administrador de IDP comprobó que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.
- Un administrador comprobó que los relojes del servidor de IDP y de la controladora están sincronizados (ya sea mediante un servidor NTP o mediante el ajuste de la configuración del reloj de la controladora).
- Se descargó un archivo de metadatos de IDP del sistema de IDP y ese archivo está disponible en el sistema local que se usa para acceder a System Manager.

Acerca de esta tarea

En esta tarea, se carga un archivo de metadatos desde IDP en System Manager. El sistema IDP necesita los metadatos para redirigir las solicitudes de autenticación a la URL correcta y validar las respuestas recibidas. Solamente es necesario cargar un solo archivo de metadatos para la cabina de almacenamiento, incluso si hay dos controladoras.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. Seleccione la pestaña **SAML**.

La página muestra información general de los pasos de configuración.

3. Haga clic en el enlace **Import Identity Provider (IDP) file**.

Se abre el cuadro de diálogo **Importar archivo del proveedor de identidades**.

4. Haga clic en **examinar** para seleccionar y cargar el archivo de metadatos IDP que copió en el sistema local.

Una vez seleccionado el archivo, se muestra el ID de entidad IDP.

5. Haga clic en **Importar**.

Paso 2: Exporte los archivos del proveedor de servicios

Para establecer una relación de confianza entre IDP y la cabina de almacenamiento, se deben importar los metadatos del proveedor de servicios en IDP.

Antes de empezar

- Conoce la dirección IP o el nombre de dominio de cada controladora de la cabina de almacenamiento.

Acerca de esta tarea

En esta tarea, es posible exportar metadatos de las controladoras (un archivo para cada controladora). IDP necesita estos metadatos para establecer una relación de confianza con las controladoras y procesar las solicitudes de autorización. El archivo incluye información, como el nombre de dominio de la controladora o la dirección IP, por lo que IDP se puede comunicar con los proveedores de servicios.

Pasos

1. Haga clic en el enlace **Exportar archivos del proveedor de servicios**.

Se abre el cuadro de diálogo **Exportar archivos del proveedor de servicios**.

2. Introduzca la dirección IP del controlador o el nombre DNS en el campo **controladora A** y, a continuación, haga clic en **Exportar** para guardar el archivo de metadatos en el sistema local. Si la matriz de almacenamiento incluye dos controladoras, repita este paso con la segunda controladora en el campo **controladora B**.

Después de hacer clic en **Exportar**, los metadatos del proveedor de servicios se descargan en el sistema local. Anote en qué lugar se almacena el archivo.

3. Desde el sistema local, busque los archivos de metadatos del proveedor de servicios que exportó.

Hay un archivo con formato XML por controladora.

4. Desde el servidor IDP, importe los archivos de metadatos del proveedor de servicios para establecer la relación de confianza. Es posible importar los archivos directamente o bien introducir manualmente la información de la controladora desde los archivos.

Paso 3: Asignar roles

Para proporcionar autorización y acceso a System Manager a los usuarios, se deben asignar los atributos de usuario IDP y las membresías de grupo a los roles predefinidos de la cabina de almacenamiento.

Antes de empezar

- Un administrador IDP configuró los atributos del usuario y la pertenencia al grupo en el sistema IDP.
- Se importó el archivo de metadatos de IDP a System Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para cada controladora en el sistema IDP.

Acerca de esta tarea

En esta tarea, se deberá usar System Manager para asignar los grupos de IDP a los roles de los usuarios locales.

Pasos

1. Haga clic en el enlace para asignar los roles de System Manager.

Se abre el cuadro de diálogo asignación de roles.

2. Asigne los grupos y atributos de usuario IDP a los roles predefinidos. Un grupo puede tener varios roles asignados.

Detalles del campo

Ajuste	Descripción
Asignaciones	Atributo de usuario
Especifique un atributo (por ejemplo, "miembro de") para el grupo SAML que será asignado.	Valor de atributo
Especifique el valor de atributo para el grupo que será asignado.	Funciones



El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

3. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.



Es posible modificar las asignaciones de roles después de haber habilitado SAML.

4. Cuando termine de asignar, haga clic en **Guardar**.

Paso 4: Probar el inicio de sesión SSO

Para garantizar la comunicación entre el sistema IDP y la cabina de almacenamiento, de manera opcional, se puede probar un inicio de sesión SSO. Esa prueba también se puede llevar a cabo durante el paso final para habilitar SAML.

Antes de empezar

- Se importó el archivo de metadatos de IDP a System Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para cada controladora en el sistema IDP.

Pasos

1. Seleccione el enlace **probar inicio de sesión SSO**.

Se abre un cuadro de diálogo para introducir las credenciales de SSO.

2. Introduzca las credenciales de inicio de sesión para un usuario, tanto con permisos de administración de

seguridad como de supervisión.

Se abre un cuadro de diálogo mientras el sistema prueba el inicio de sesión.

3. Busque el mensaje Test Successful. Si el análisis se realiza correctamente, vaya al siguiente paso para habilitar SAML.

Si el análisis no se realiza correctamente, se muestra un mensaje de error con más información. Asegúrese de que:

- El usuario pertenezca a un grupo con permisos de administración de seguridad y supervisión.
- Los metadatos cargados para el servidor IDP sean correctos.
- Las direcciones de las controladoras en los archivos de metadatos de SP sean correctas.

Paso 5: Habilite SAML

El paso final es habilitar la autenticación de usuario SAML.

Antes de empezar

- Se importó el archivo de metadatos de IDP a System Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para cada controladora en el sistema IDP.
- Se debe configurar al menos una asignación de rol de administración de seguridad y una de rol de supervisión.

Acerca de esta tarea

En esta tarea, se describe cómo completar la configuración de SAML para la autenticación de usuarios. Durante este proceso, el sistema también le indica que pruebe un inicio de sesión SSO. El proceso de prueba de inicio de sesión con SSO se describe en el paso anterior.



Edición y desactivación. una vez que SAML está habilitado, *no puede* desactivarlo a través de la interfaz de usuario, ni puede editar la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

Pasos

1. En la ficha **SAML**, seleccione el enlace **Habilitar SAML**.

Se abre el cuadro de diálogo **Confirmar activación de SAML**.

2. Tipo `enable` Y, a continuación, haga clic en **Activar**.
3. Introduzca las credenciales de usuario para llevar a cabo una prueba de inicio de sesión SSO.

Resultados

Una vez que el sistema habilita SAML, se cierran todas las sesiones activas y se inicia la autenticación de usuarios a través de SAML.

Cambiar las asignaciones de roles SAML

Si anteriormente configuró SAML para Access Management, puede cambiar las asignaciones de roles entre los grupos IDP y los roles predefinidos de la cabina de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Un administrador IDP configuró los atributos del usuario y la pertenencia al grupo en el sistema IDP.
- SAML debe estar configurado y habilitado.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. Seleccione la pestaña **SAML**.
3. Seleccione **asignación de roles**.

Se abre el cuadro de diálogo **asignación de roles**.

4. Asigne los grupos y atributos de usuario IDP a los roles predefinidos. Un grupo puede tener varios roles asignados.



Tenga cuidado de no quitar los permisos mientras SAML está habilitado; de lo contrario, perderá el acceso a System Manager.

Detalles del campo

Ajuste	Descripción
Asignaciones	Atributo de usuario
Especifique un atributo (por ejemplo, "miembro de") para el grupo SAML que será asignado.	Valor de atributo
Especifique el valor de atributo para el grupo que será asignado.	Funciones



El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

1. **Opcional:** haga clic en **Añadir otra asignación** para introducir más asignaciones de grupo a rol.
2. Haga clic en **Guardar**.

Resultados

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Exporte los archivos de proveedor de servicios SAML

Si es necesario, se pueden exportar metadatos de proveedor de servicios para la cabina de almacenamiento y volver a importar los archivos en el sistema del proveedor de identidades (IDP).

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- SAML debe estar configurado y habilitado.

Acerca de esta tarea

En esta tarea, es posible exportar metadatos de las controladoras (un archivo para cada controladora). IDP necesita estos metadatos para establecer una relación de confianza con las controladoras y procesar solicitudes de autenticación. El archivo incluye información, como el nombre de dominio o la dirección IP de la controladora, que IDP puede usar para enviar solicitudes.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. Seleccione la pestaña **SAML**.
3. Seleccione **Exportar**.

Se abre el cuadro de diálogo **Exportar archivos del proveedor de servicios**.

4. Para cada controlador, haga clic en **Exportar** para guardar el archivo de metadatos en el sistema local.



Los campos de nombre de dominio para cada controladora son de solo lectura.

Anote en qué lugar se almacena el archivo.

5. Desde el sistema local, busque los archivos de metadatos del proveedor de servicios que exportó.

Hay un archivo con formato XML por controladora.

6. Desde el servidor IDP, importe los archivos de metadatos del proveedor de servicios. Puede importar los archivos directamente o introducir manualmente la información de la controladora incluida en ellos.
7. Haga clic en **Cerrar**.

Ver actividad de registro de auditoría

Al ver los registros de auditoría, los usuarios que tienen permisos de administrador de seguridad pueden supervisar acciones de usuarios, fallos de autenticación, intentos de inicio de sesión no válidos y la vida útil de la sesión de usuario.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.




2. Seleccione la ficha **Registro de auditoría**.

La actividad de registro de auditoría aparece en una tabla de resultados, que incluye las siguientes columnas de información:

- **Fecha/Hora** — Marca de hora del momento en que la matriz de almacenamiento detectó el evento (en GMT).
- **Nombre de usuario** — el nombre de usuario asociado al evento. Para cualquier acción sin autenticar en la cabina de almacenamiento, aparece "N/A" como nombre de usuario. El proxy interno o algún otro mecanismo podrían activar acciones sin autenticar.
- **Código de estado** — Código de estado HTTP de la operación (200, 400, etc.) y texto descriptivo asociado al evento.
- **URL visitada** — URL completa (incluido el host) y cadena de consulta.
- **Dirección IP del cliente** — Dirección IP del cliente asociado al evento.
- **Source** — origen de registro asociado al evento, que puede ser System Manager, CLI, Web Services o Support Shell.

3. Use las selecciones de la página Registro de auditoría para ver y gestionar eventos.

Detalles de selección

Selección	Descripción
Mostrar eventos de...	Eventos de límite mostrados por rango de fechas (últimas 24 horas, últimos 7 días, últimos 30 días o un rango de fechas personalizado).
Filtro	Eventos de límite mostrados por los caracteres introducidos en el campo. Utilice comillas (") para una coincidencia exacta de palabras, introduzca OR para devolver una o más palabras, o introduzca un guión (--) para omitir palabras.
Actualice	Seleccione Actualizar para actualizar la página a los eventos más recientes.
Ver/editar configuración	Seleccione Ver/editar configuración para abrir un cuadro de diálogo que permite especificar una política de registro completo y el nivel de acciones que se registrarán.
Eliminar eventos	Seleccione Eliminar para abrir un cuadro de diálogo que le permite eliminar eventos antiguos de la página.
Mostrar/ocultar columnas	<p>Haga clic en el icono de la columna Mostrar/Ocultar  para seleccionar columnas adicionales para mostrar en la tabla. Las columnas adicionales incluyen:</p> <ul style="list-style-type: none"> • Método — el método HTTP (POR ejemplo, POST, GET, DELETE, etc.). • Comando CLI ejecutado — el comando CLI (gramática) ejecutado para solicitudes Secure CLI. • Estado de devolución de CLI — un código de estado de CLI o una solicitud de archivos de entrada del cliente. • Procedimiento de Symbol — procedimiento de Symbol ejecutado. • Tipo de evento SSH — Tipo de eventos Secure Shell (SSH), como inicio de sesión, cierre de sesión y login_fail. • PID de sesión SSH — número de ID de proceso de la sesión SSH. • Duración(s) de sesión de SSH — el número de segundos en los que el usuario estuvo conectado.
Alternar filtros de columnas	Haga clic en el icono alternar  para abrir los campos de filtrado de cada columna. Introduzca los caracteres en un campo de columna para limitar los eventos que se muestran con esos caracteres. Vuelva a hacer clic en el icono para cerrar los campos de filtrado.
Deshacer cambios	Haga clic en el icono Deshacer  para devolver la tabla a la configuración predeterminada.

Selección	Descripción
Exportar	Haga clic en Exportar para guardar los datos de la tabla en un archivo de valores separados por comas (CSV).

Defina políticas de registro de auditoría

Es posible cambiar la política de sobrescritura y los tipos de eventos registrados en el registro de auditoría.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

En esta tarea, se describe la forma de cambiar la configuración del registro de auditoría, lo que incluye la política para sobrescribir eventos anteriores y la política para registrar tipos de eventos.



Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. Seleccione la ficha **Registro de auditoría**.
3. Seleccione **Ver/editar configuración**.

Se abrirá el cuadro de diálogo **Configuración del registro de auditoría**.

4. Cambie la política de sobrescritura o los tipos de eventos registrados.

Detalles del campo

Ajuste	Descripción
Política de sobrescritura	<p>Determine la política para sobrescribir eventos antiguos cuando se alcanza la capacidad máxima:</p> <ul style="list-style-type: none"> • Permitir que los eventos más antiguos del registro de auditoría se sobrescriban cuando el registro de auditoría está lleno — sobrescribe los eventos antiguos cuando el registro de auditoría llega a 50,000 registros. • Requerir que se eliminen manualmente los eventos del registro de auditoría — especifica que los eventos no se eliminarán automáticamente; en su lugar, aparecerá una advertencia de umbral en el porcentaje establecido. Los eventos deben eliminarse manualmente. <div>  Si se deshabilita la política de sobrescritura y las entradas del registro de auditoría llegan al límite máximo, se deniega el acceso a System Manager para usuarios sin permisos de Administrador de seguridad. Para restaurar el acceso al sistema para usuarios sin permisos de Administrador de seguridad, un usuario asignado al rol Security Admin debe eliminar los registros de eventos anteriores. </div> <div>  Las políticas de sobrescritura no se aplican si un servidor de syslog está configurado para archivar registros de auditoría. </div>
Nivel de acciones que se registrarán	<p>Determina los tipos de eventos que deben registrarse:</p> <ul style="list-style-type: none"> • Grabar sólo eventos de modificación — muestra sólo los eventos en los que una acción del usuario implica realizar un cambio en el sistema. • Grabar todos los eventos de modificación y sólo lectura — muestra todos los eventos, incluyendo una acción del usuario que implica leer o descargar información.

5. Haga clic en **Guardar**.

Elimine eventos del registro de auditoría

Es posible borrar los eventos antiguos del registro de auditoría para que la búsqueda de eventos sea más sencilla. Tiene la opción de guardar los eventos antiguos en un archivo CSV (valores separados por comas) después de su eliminación.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

En esta tarea, se describe la forma de eliminar eventos antiguos del registro de auditoría.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. Seleccione la ficha **Registro de auditoría**.
3. Seleccione **Eliminar**.

Se abre el cuadro de diálogo Eliminar registro de auditoría.

4. Seleccione o escriba el número de eventos antiguos que desea eliminar.
5. Si desea exportar los eventos eliminados a un archivo CSV (recomendado), mantenga seleccionada la casilla de comprobación. Se le pedirá que introduzca un nombre de archivo y una ubicación al hacer clic en **Eliminar** en el paso siguiente. De lo contrario, si no desea guardar eventos en un archivo CSV, haga clic en la casilla de comprobación para cancelar la selección.
6. Haga clic en **Eliminar**.

Se abre un cuadro de diálogo de confirmación.

7. Tipo `delete` En el campo y, a continuación, haga clic en **Eliminar**.

Los eventos más antiguos se eliminarán de la página Registro de auditoría.

Configurar servidores de syslog para registros de auditoría

Si desea archivar registros de auditoría en un servidor de syslog externo, puede configurar las comunicaciones entre ese servidor y la cabina de almacenamiento. Una vez que se establece la conexión, los registros de auditoría se guardan automáticamente en el servidor de syslog.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- La dirección, el protocolo y el número de puerto del servidor de syslog deben estar disponibles. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si el servidor usa un protocolo seguro (por ejemplo, TLS), debe haber disponible un certificado de entidad de certificación (CA) en el sistema local. Los certificados DE CA identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. En la ficha **Registro de auditoría**, seleccione **Configurar servidores de syslog**.

Se abre el cuadro de diálogo **Configurar servidores de syslog**.

3. Haga clic en **Agregar**.

Se abrirá el cuadro de diálogo **Agregar servidor de syslog**.

4. Introduzca la información del servidor y, a continuación, haga clic en **Agregar**.

- **Dirección del servidor** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- **Protocolo** — Seleccione un protocolo de la lista desplegable (por ejemplo, TLS, UDP o TCP).
- **Cargar certificado (opcional)** — Si ha seleccionado el protocolo TLS y todavía no ha cargado un certificado de CA firmado, haga clic en **examinar** para cargar un archivo de certificado. Los registros de auditoría no se archivan en un servidor de syslog si no cuentan con un certificado de confianza.



Si la certificación ya no es válida en el futuro, el apretón de manos de TSL fallará. Como resultado, se publica un mensaje de error en el registro de auditoría y ya no se envían mensajes al servidor de syslog. Para resolver este problema, debe corregir el certificado en el servidor syslog y, a continuación, ir a **menú:Configuración[Registro de auditoría > Configurar servidores Syslog > probar todo]**.

- **Puerto** — Introduzca el número de puerto para el receptor de syslog.

Después de hacer clic en **Agregar**, se abre el cuadro de diálogo **Configurar servidores de syslog** y se muestra el servidor de syslog configurado en la página.

5. Para probar la conexión del servidor con la matriz de almacenamiento, seleccione **probar todo**.

Resultados

Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren.

Editar la configuración del servidor de syslog para los registros de auditoría

Es posible modificar la configuración del servidor de syslog utilizada para archivar registros de auditoría, y también cargar un nuevo certificado de una entidad de certificación (CA) para el servidor.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- La dirección, el protocolo y el número de puerto del servidor de syslog deben estar disponibles. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si va a cargar un nuevo certificado de CA, el certificado debe estar disponible en el sistema local.

Pasos

1. Seleccione **MENU:Settings[Access Management]**.
2. En la ficha **Registro de auditoría**, seleccione **Configurar servidores de syslog**.

Los servidores de syslog configurados se muestran en la página.

3. Para editar la información del servidor, seleccione el icono **Editar** (lápiz) situado a la derecha del nombre del servidor y, a continuación, realice los cambios deseados en los siguientes campos:
 - **Dirección del servidor** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.

- **Protocolo** — Seleccione un protocolo de la lista desplegable (por ejemplo, TLS, UDP o TCP).
 - **Puerto** — Introduzca el número de puerto para el receptor de syslog.
4. Si cambió el protocolo al protocolo TLS seguro (desde UDP o TCP), haga clic en **Importar certificado de confianza** para cargar un certificado de CA.
 5. Para probar la nueva conexión con la matriz de almacenamiento, seleccione **probar todo**.

Resultados

Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren.

Preguntas frecuentes

¿Por qué no puedo iniciar sesión?

Si recibe un error al intentar iniciar sesión en System Manager, revise estas causas posibles.

Los errores de inicio de sesión en System Manager pueden ocurrir por uno de estos motivos:

- Introdujo un nombre de usuario o contraseña incorrectos.
- No tiene privilegios suficientes.
- El servidor de directorio (si está configurado) puede no estar disponible. Si este es el caso, intente iniciar sesión con un rol de usuario local.
- Intentó iniciar sesión reiteradamente sin éxito y se activó el modo de bloqueo. Espere 10 minutos y vuelva a intentarlo.
- Se activó la condición de bloqueo y es posible que el registro de auditoría esté completo. Vaya a Access Management y elimine los eventos anteriores del registro de auditoría.
- La autenticación SAML está habilitada. Actualice el explorador para iniciar sesión.

Los errores de inicio de sesión en una cabina de almacenamiento remota para tareas de mirroring pueden ocurrir por uno de estos motivos:

- Introdujo una contraseña incorrecta.
- Intentó iniciar sesión reiteradamente sin éxito y se activó el modo de bloqueo. Espere 10 minutos para volver a iniciar sesión.
- Se alcanzó la cantidad máxima de conexiones de clientes en la controladora. Busque clientes o usuarios múltiples.

¿Qué debo saber antes de añadir un servidor de directorio?

Antes de añadir un servidor de directorio en Access Management, asegúrese de cumplir con los siguientes requisitos.

- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.
- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

¿Qué debo saber acerca de la asignación de roles de la cabina de almacenamiento?

Antes de asignar grupos a roles, revise las siguientes directrices.

Las funcionalidades de control de acceso basado en roles (RBAC) incorporadas en la cabina de almacenamiento incluyen los siguientes roles:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento (por ejemplo, volúmenes y pools de discos), pero sin acceso a la configuración de seguridad.
- **Administración de seguridad** — acceso a la configuración de seguridad en Access Management, administración de certificados, administración de registros de auditoría y la capacidad de activar o desactivar la interfaz de administración heredada (Symbol).
- **Support admin** — acceso a todos los recursos de hardware en la cabina de almacenamiento, datos de fallos, eventos MEL y actualizaciones del firmware de la controladora. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Servicios de directorio

Si usa un servidor de protocolo ligero de acceso a directorios (LDAP) y servicios de directorio, asegúrese de que:

- Un administrador haya definido grupos de usuarios en el servicio de directorio.
- Conoce los nombres de dominio de los grupos de usuarios LDAP.
- El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

SAML

Si usa las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) incorporadas en la cabina de almacenamiento, asegúrese de que:

- Un administrador de proveedor de identidades (IDP) haya configurado atributos de usuario y pertenencia a grupos en el sistema del IDP.
- Conoce los nombres de pertenencia a grupos.
- El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

¿A cuáles herramientas de gestión externas puede afectar este cambio?

Cuando se realizan ciertos cambios en System Manager, como el cambio de la interfaz de gestión o el uso de SAML como método de autenticación, puede restringirse el uso de algunas herramientas y funciones externas.

Interfaz de gestión

Las herramientas que se comunican directamente con la interfaz de gestión heredada (Symbol), como SANtricity SMI-S Provider u OnCommand Insight (OCI), no funcionan a menos que la configuración interfaz de gestión heredada esté habilitada. Además, no es posible utilizar comandos de la CLI heredados ni realizar operaciones de mirroring si dicha configuración está deshabilitada.

Póngase en contacto con el soporte técnico para obtener más información.

Autenticación SAML

Cuando se habilita SAML, los siguientes clientes no pueden acceder a los recursos y los servicios de la cabina de almacenamiento:

- Enterprise Management Window (EMW)
- Interfaz de línea de comandos (CLI)
- Clientes de kits de desarrollo de software (SDK)
- Clientes en banda
- Clientes HTTP de la API de REST de autenticación básica
- Inicio de sesión mediante extremo estándar de la API de REST

Póngase en contacto con el soporte técnico para obtener más información.

¿Qué debo saber antes de configurar y habilitar SAML?

Antes de configurar y habilitar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) para la autenticación, asegúrese de cumplir con los siguientes requisitos y comprender las restricciones de SAML.

Requisitos

Antes de comenzar, compruebe lo siguiente:

- Se configuró un proveedor de identidades (IDP) en la red. Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. El equipo de seguridad es responsable de mantener el IDP.
- Un administrador IDP configuró los atributos y los grupos del usuario en el sistema IDP.
- Un administrador de IDP comprobó que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.
- Un administrador comprobó que los relojes del servidor de IDP y de la controladora están sincronizados (ya sea mediante un servidor NTP o mediante el ajuste de la configuración del reloj de la controladora).
- Se descargó un archivo de metadatos de IDP del sistema de IDP y ese archivo está disponible en el sistema local que se usa para acceder a System Manager.
- Conoce la dirección IP o el nombre de dominio de cada controladora de la cabina de almacenamiento.

Restricciones

Además de los requisitos mencionados más arriba, asegúrese de comprender las siguientes restricciones:

- Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda. Se recomienda que pruebe los inicios de sesión SSO para poder habilitar SAML en el paso final de la configuración. (El sistema también hace una prueba de inicio de sesión SSO antes de habilitar SAML.)
- Si deshabilita SAML en el futuro, el sistema restaura automáticamente la configuración anterior (local User roles o Directory Services).

- Si Directory Services está actualmente configurado para la autenticación de usuario, SAML anula esa configuración.
- Cuando se configura SAML, los siguientes clientes no pueden acceder a los recursos de la cabina de almacenamiento:
 - Enterprise Management Window (EMW)
 - Interfaz de línea de comandos (CLI)
 - Clientes de kits de desarrollo de software (SDK)
 - Clientes en banda
 - Clientes HTTP de la API de REST de autenticación básica
 - Inicio de sesión mediante extremo estándar de la API de REST

¿Qué tipo de eventos se registran en el registro de auditoría?

El registro de auditoría puede incluir eventos de modificación, o bien tanto eventos de modificación como de solo lectura.

Según la configuración de la política, se muestran los siguientes tipos de eventos:

- **Eventos de modificación** — acciones del usuario desde System Manager que involucran cambios en el sistema, como el aprovisionamiento de almacenamiento.
- **Eventos de modificación y de sólo lectura** — acciones del usuario que involucran cambios en el sistema, así como eventos que involucran la visualización o descarga de información, como la visualización de asignaciones de volumen.

¿Qué debo saber antes de configurar un servidor de syslog?

Es posible archivar registros de auditoría en un servidor de syslog externo.

Antes de configurar un servidor de syslog, tenga en cuenta las siguientes directrices.

- Asegúrese de conocer la dirección, el protocolo y el número de puerto del servidor. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si el servidor usa un protocolo seguro (por ejemplo, TLS), debe haber disponible un certificado de entidad de certificación (CA) en el sistema local. Los certificados DE CA identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes.
- Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren.
- La configuración de la política de sobrescritura (disponible en **View/Edit Settings**) no afecta a la forma en que se gestionan los registros con una configuración de servidor syslog.
- Los registros de auditoría tienen el formato de mensajería RFC 5424.

El servidor de syslog ya no recibe registros de auditoría. ¿Qué debo hacer?

Si configuró un servidor de syslog con un protocolo TLS, el servidor no puede recibir mensajes si la certificación no es válida por algún motivo. Se envía un mensaje de error sobre el certificado no válido al registro de auditoría.

Para resolver este problema, debe corregir la certificación para el servidor de syslog. Una vez que haya una

cadena de certificados válida en su lugar, vaya a **menú:Configuración[Registro de auditoría > Configurar servidores de syslog > probar todo]**.

Certificados

Conceptos

Cómo funcionan los certificados

Los certificados son archivos digitales que identifican entidades en línea, como sitios web y servidores, para poder establecer comunicaciones seguras en Internet.

Los certificados garantizan que solo se transmitan comunicaciones web en formato cifrado, de forma privada y sin alternaciones, entre el servidor especificado y el cliente. Con System Manager, puede gestionar los certificados entre el explorador en un sistema de gestión host (que actúa como cliente) y las controladoras en un sistema de almacenamiento (que actúan como servidores).

Un certificado puede estar firmado por una autoridad de confianza o puede ser autofirmado. La firma simplemente implica que alguien validó la identidad del propietario y determinó que sus dispositivos son de confianza. Las cabinas de almacenamiento se entregan con un certificado autofirmado generado automáticamente en cada controladora. Puede continuar usando el certificado autofirmado o puede obtener certificados firmados por CA para establecer conexiones más seguras entre las controladoras y los sistemas host.



Si bien los certificados firmados por CA aumentan la protección de seguridad (por ejemplo, evitan los ataques de tipo "man in the middle"), también aplican tarifas que pueden ser costosas si la red es extensa. En cambio, los certificados autofirmados son menos seguros, pero son gratuitos. Por lo tanto, los certificados autofirmados se utilizan con mayor frecuencia para entornos de prueba internos, no en entornos de producción.

Certificados firmados

Un certificado firmado es validado por una entidad de certificación (CA), que es una organización de terceros de confianza. Los certificados firmados incluyen detalles sobre el propietario de la entidad (generalmente, un servidor o sitio web), la fecha de emisión y de vencimiento del certificado, los dominios válidos de la entidad, y una firma digital compuesta por letras y números.

Al abrir un explorador y escribir una dirección web, el sistema ejecuta un proceso de comprobación de certificados en segundo plano para determinar si el usuario se está conectando a un sitio web que incluye un certificado válido firmado por una CA. Generalmente, un sitio que está protegido con un certificado firmado incluye un icono de candado y una designación https en la dirección. Si el usuario intenta conectarse a un sitio web que no contiene un certificado firmado por CA, el explorador mostrará una advertencia para indicar que el sitio no es seguro.

La CA toma las medidas necesarias para verificar las identidades durante el proceso de solicitud. La entidad puede enviar un correo electrónico a la empresa registrada, verificar la dirección empresarial, y realizar una verificación de HTTP o DNS. Una vez completado el proceso de solicitud, la CA envía los archivos digitales para cargar en el sistema de gestión host. Normalmente, estos archivos contienen una cadena de confianza como la siguiente:

- **Raíz:** En la parte superior de la jerarquía se encuentra el certificado raíz, que contiene una clave privada que se utiliza para firmar otros certificados. El certificado raíz identifica una organización de CA determinada. Si utiliza la misma CA para todos los dispositivos de red, solo necesita un certificado raíz.

- Intermedio: Como una rama del certificado raíz, se encuentran los certificados intermedios. La CA emite uno o varios certificados intermedios para actuar como intermediarios entre un certificado raíz y los certificados de servidor protegidos.
- Servidor: En la parte inferior de la cadena se encuentra el certificado de servidor, que identifica la entidad específica del usuario, como un sitio web u otro dispositivo. Cada controladora de una cabina de almacenamiento requiere un certificado de servidor aparte.

Certificados autofirmados

Cada controladora de la cabina de almacenamiento incluye un certificado autofirmado preinstalado. Un certificado autofirmado es similar a un certificado firmado por CA, excepto que es validado por el propietario de la entidad y no por un tercero. Al igual que un certificado firmado por CA, un certificado autofirmado contiene su propia clave privada, y también garantiza que los datos se cifren y se envíen a través de una conexión HTTPS entre un servidor y un cliente. Sin embargo, un certificado autofirmado no utiliza la misma cadena de confianza que un certificado firmado por CA.

Los certificados autofirmados no son «'de confianza'» por parte de los navegadores. Cada vez que intente conectarse a un sitio web que solo contiene un certificado autofirmado, el explorador mostrará un mensaje de advertencia. Deberá hacer clic en un enlace del mensaje de advertencia para continuar al sitio web; al hacer eso, estará aceptando básicamente el certificado autofirmado.

Certificados usados para el servidor de gestión de claves

Si usa un servidor de gestión de claves externo con la función Drive Security, también puede gestionar los certificados para la autenticación entre ese servidor y las controladoras.

Terminología de certificados

Los siguientes términos se utilizan en la gestión de certificados.

Duración	Descripción
APROX	Una entidad de certificación (CA) es una entidad de confianza que emite documentos electrónicos, denominados certificados digitales, para la seguridad de Internet. Estos certificados identifican a los propietarios de sitios web y, de esta manera, permiten conexiones seguras entre clientes y servidores.
CSR	Una solicitud de firma de certificación (CSR) es un mensaje que envía un solicitante a una entidad de certificación (CA). La CSR valida la información que requiere la CA para emitir un certificado.
Certificado	Un certificado identifica al propietario de un sitio con el fin de brindar seguridad, para evitar que atacantes se hagan pasar por los propietarios del sitio. El certificado tiene información acerca del propietario del sitio y la identidad de la entidad de confianza que certifica (firma) esta información.
Cadena de certificados	La cadena de certificados es una jerarquía de archivos que suma una capa de seguridad a los certificados. Normalmente, la cadena incluye un certificado raíz en la parte superior de la jerarquía, uno o varios certificados intermedios y los certificados de servidor que identifican a las entidades.

Duración	Descripción
Certificado de cliente	En la gestión de claves de seguridad, un certificado de cliente valida las controladoras de la cabina de almacenamiento a fin de que el servidor de gestión de claves pueda confiar en sus direcciones IP.
Certificado intermedio	Uno o varios certificados intermedios se extienden como una rama del certificado raíz en la cadena de certificados. La CA emite uno o varios certificados intermedios para actuar como intermediarios entre un certificado raíz y los certificados de servidor protegidos.
Certificado de servidor de gestión de claves	En la gestión de claves de seguridad, un certificado de servidor de gestión de claves valida el servidor a fin de que la cabina de almacenamiento pueda confiar en su dirección IP.
Almacén de claves	Un almacén de claves es un repositorio en el sistema de gestión host que contiene claves privadas, junto con sus correspondientes claves públicas y certificados. Estas claves y certificados identifican a las entidades propias como, por ejemplo, las controladoras.
Servidor OCSP	El servidor de protocolo de estado de certificado en línea (OCSP) determina si la entidad de certificación (CA) ha revocado algún certificado antes de su fecha de vencimiento programada y bloquea el acceso del usuario a un servidor si se ha revocado el certificado.
Certificado raíz	El certificado raíz se encuentra en la parte superior de la jerarquía de la cadena de certificados y contiene una clave privada que se utiliza para firmar otros certificados. El certificado raíz identifica una organización de CA determinada. Si utiliza la misma CA para todos los dispositivos de red, solo necesita un certificado raíz.
Certificado firmado	Un certificado que ha validado una entidad de certificación (CA). Este archivo de datos contiene una clave privada, y garantiza que los datos se envíen en formato cifrado entre un servidor y un cliente a través de una conexión HTTPS. Además, un certificado firmado incluye detalles sobre el propietario de la entidad (normalmente, un servidor o sitio web) y una firma digital compuesta por letras y números. Un certificado firmado usa una cadena de certificados y, por consiguiente, se utiliza con mayor frecuencia en los entornos de producción. También se conoce como "certificado firmado por CA" o "certificado de gestión".
Certificado autofirmado	Un certificado autofirmado es validado por el propietario de la entidad. Este archivo de datos contiene una clave privada, y garantiza que los datos se envíen en formato cifrado entre un servidor y un cliente a través de una conexión HTTPS. También incluye una firma digital compuesta por letras y números. Un certificado autofirmado no usa la misma cadena de confianza que un certificado firmado por CA y, por consiguiente, se utiliza con mayor frecuencia en los entornos de prueba. También se conoce como certificado "preinstalado".

Duración	Descripción
Certificado de servidor	El certificado de servidor se encuentra en la parte inferior de la cadena de certificados. Este certificado identifica la entidad específica del usuario, por ejemplo, un sitio web u otro dispositivo. Cada controladora de un sistema de almacenamiento requiere un certificado de servidor aparte.

Procedimientos

Use certificados firmados por CA para las controladoras

Es posible obtener certificados firmados por CA para establecer comunicaciones seguras entre las controladoras y el explorador que se utiliza para acceder a System Manager.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Acerca de esta tarea

El uso de certificados firmados por CA implica un procedimiento de tres pasos.

Paso 1: Complete y envíe una CSR para las controladoras

Primero, es necesario generar un archivo de solicitud de firma de certificación (CSR) para cada controladora de la cabina de almacenamiento y, a continuación, enviar los archivos a la entidad de certificación (CA).

Antes de empezar

- Debe conocer la dirección IP o el nombre DNS de cada controladora.

Acerca de esta tarea

La CSR proporciona información sobre su organización, la dirección IP o el nombre DNS de la controladora, y una pareja de claves para identificar el servidor web de la controladora. Durante esta tarea, se genera un archivo CSR si solo existe una controladora en la cabina de almacenamiento y dos archivos CSR si existen dos controladoras.



No genere una nueva CSR después de enviar una a la CA. Al generar una CSR, el sistema crea una pareja de claves pública y privada. La clave pública se incluye en la CSR, mientras que la clave privada se conserva en el almacén de claves. Al recibir los certificados firmados e importarlos al almacén de claves, el sistema se asegura de que las claves pública y privada sean la pareja original. Por lo tanto, no debe generar una nueva CSR después de enviar una a la CA. Si lo hace, las controladoras generarán claves nuevas y los certificados que reciba de la CA no funcionarán.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Gestión de matrices**, seleccione **completar CSR**.



Si aparece un cuadro de diálogo que le pide que acepte un certificado autofirmado para el segundo controlador, haga clic en **Aceptar certificado autofirmado** para continuar.

3. Introduzca la siguiente información y, a continuación, haga clic en **Siguiente**:

- **Organización** — el nombre completo y legal de su empresa u organización. Incluya sufijos, como Inc. O Corp
- **Unidad organizativa (opcional)** — la división de su organización que maneja el certificado.
- **Ciudad/localidad** — Ciudad en la que se encuentra la matriz de almacenamiento o el negocio.
- **Estado/Región (opcional)** — el estado o región donde está ubicada la matriz de almacenamiento o el negocio.
- **Código ISO de país:** Código ISO (Organización Internacional de Normalización) de dos dígitos de su país, por ejemplo, US.



Algunos campos pueden autocompletarse con la información adecuada, como la dirección IP de la controladora. No cambie los valores autocompletados a menos que esté seguro de que son incorrectos. Por ejemplo, si todavía no ha completado una CSR, la dirección IP de la controladora se establecerá en "localhost". En ese caso, deberá cambiar «'localhost'» por el nombre DNS o la dirección IP del controlador.

4. Verifique o introduzca la siguiente información acerca de la controladora A en su cabina de almacenamiento:

- **Controller un nombre común** — la dirección IP o el nombre DNS del controlador A se muestran de manera predeterminada. Compruebe que la dirección sea correcta; debe coincidir exactamente con lo que escribe para acceder a System Manager en el explorador.
- **Controller a Alternate IP address** — Si el nombre común es una dirección IP, puede opcionalmente escribir cualquier dirección IP adicional o alias para el controlador A. Si va a introducir varios datos, use un formato delimitado por comas.
- **Nombre DNS alternativo del controlador a** — Si el nombre común es un nombre DNS, introduzca cualquier nombre DNS adicional para el controlador A. Si va a introducir varios datos, use un formato delimitado por comas. Si no hay nombres DNS alternativos, pero especificó un nombre DNS en el primer campo, copie ese nombre aquí. Si la cabina de almacenamiento sólo tiene una controladora, el botón **Finalizar** estará disponible. Si la cabina de almacenamiento tiene dos controladores, el botón **Siguiente** estará disponible.



No haga clic en el enlace **Omitir este paso** cuando cree inicialmente una solicitud CSR. El enlace se proporciona para situaciones de recuperación de errores. En raras ocasiones, una solicitud CSR puede generar errores en una controladora, pero no en la otra. Este enlace permite omitir el paso para crear una solicitud CSR en la controladora A si ya está definida, y continuar hacia el siguiente paso para volver a crear una solicitud CSR en la controladora B.

5. Si sólo hay un controlador, haga clic en **Finalizar**. Si hay dos controladores, haga clic en **Siguiente** para introducir información para el controlador B (igual que el anterior) y, a continuación, haga clic en **Finalizar**.

Para una sola controladora, se descarga un archivo CSR en el sistema local. Para controladoras dobles, se descargan dos archivos CSR. La ubicación de la carpeta de la descarga depende del explorador.

6. Busque los archivos CSR descargados. La ubicación de la carpeta depende del explorador.

7. Envíe los archivos CSR a una CA y solicite certificados firmados en formato PEM.

8. Espere a que la CA devuelva los certificados y vaya a [Paso 2: Importe los certificados firmados para las controladoras](#).

Paso 2: Importe los certificados firmados para las controladoras

Después de recibir los certificados firmados, es necesario importar los archivos para las controladoras.

Antes de empezar

- La CA devolvió archivos de certificado firmados.
- Los archivos se encuentran disponibles en el sistema local.
- Si la CA proporcionó un certificado encadenado (por ejemplo, un archivo .p7b), debe desempaquetar el archivo encadenado en archivos individuales: El certificado raíz, el o los certificados intermedios y los certificados de servidor que identifican a las controladoras. Puede utilizar Windows `certmgr` Utilidad para desempaquetar los archivos (haga clic con el botón derecho y seleccione **menú: todas las tareas[Exportar]**). Una vez completadas las exportaciones, se mostrará un archivo CER para cada archivo de certificado de la cadena.

Acerca de esta tarea

En esta tarea, se describe la manera de cargar los archivos de certificado.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Administración de matrices**, seleccione **Importar**.

Se abre un cuadro de diálogo para importar los archivos de certificado.

3. Haga clic en los botones **examinar** para seleccionar primero el archivo raíz y los archivos intermedios y, a continuación, seleccionar cada certificado de servidor para los controladores. El archivo raíz y los archivos intermedios son los mismos para ambas controladoras. Solo los certificados de servidor son únicos para cada controladora.

Se muestran los nombres de los archivos en el cuadro de diálogo.

4. Haga clic en **Importar**.

Los archivos se cargan y validan.

Resultados

La sesión finaliza automáticamente. Debe volver a iniciar sesión para que los certificados entren en vigencia. Cuando inicia sesión nuevamente, se utiliza el nuevo certificado firmado por la CA en la sesión.

Restablezca los certificados de gestión

Es posible revertir los certificados que se usan en las controladoras de los certificados firmados por CA a los certificados autofirmados de fábrica.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Se deben importar de forma previa los certificados firmados por CA.

Acerca de esta tarea

La función Restablecer elimina los archivos de certificados firmados por CA actuales de cada controladora. A continuación, las controladoras reversion al uso de certificados autofirmados.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Administración de matrices**, seleccione **Restablecer**.

Se abre el cuadro de diálogo Confirmar **Restablecer certificados de administración**.

3. Tipo reset En el campo y, a continuación, haga clic en **Restablecer**.

Una vez que se actualiza el explorador, es posible que el explorador bloquee el acceso al sitio de destino e informe de que el sitio utiliza HTTP estricto Transport Security. Esta condición surge cuando se cambia a certificados autofirmados. Para borrar la condición que bloquea el acceso al destino, debe borrar los datos de navegación del explorador.

Resultados

Las controladoras revierten al uso de certificados autofirmados. Como resultado, el sistema solicita a los usuarios que acepten manualmente el certificado autofirmado para sus sesiones.

Vea información de certificaciones importadas

Desde la página certificados, es posible ver el tipo de certificado, la entidad emisora y el rango válido de fechas de los certificados para la cabina de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Pasos

1. Seleccione MENU:Settings[Certificates].
2. Seleccione una de las pestañas para ver información sobre los certificados.

Pestaña	Descripción
Gestión de cabinas	Vea información sobre los certificados firmados por CA importados para cada controladora, incluido el archivo raíz, los archivos intermedios y los archivos de servidor.
De confianza	<p>Vea información sobre los otros tipos de certificados importados para las controladoras. Utilice el campo de filtro en Mostrar certificados... para ver certificados instalados por el usuario o instalados previamente.</p> <ul style="list-style-type: none">• Instalado por el usuario. Los certificados que un usuario cargó en la cabina de almacenamiento, los cuales pueden incluir certificados de confianza cuando la controladora funciona como cliente (en lugar de servidor), certificados LDAPS y certificados de la Federación de identidades.• Preinstalado. Los certificados autofirmados incluidos con la cabina de almacenamiento.
Gestión de claves	Vea información sobre los certificados firmados por CA importados para un servidor de gestión de claves externo.

Importar certificados para las controladoras cuando funcionan como clientes

Si la controladora rechaza una conexión debido a que no puede validar la cadena de confianza de un servidor de red, es posible importar un certificado de la pestaña de confianza con el que la controladora (actuando como cliente) pueda aceptar comunicaciones de ese servidor.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Los archivos de certificado están instalados en el sistema local.

Acerca de esta tarea

Es posible que sea necesario importar certificados de la pestaña de confianza para permitir que otro servidor se comuniquen con las controladoras (por ejemplo, un servidor de syslog o un servidor LDAP que utiliza TLS).

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Trusted**, seleccione **Importar**.

Se abre un cuadro de diálogo para importar los archivos de certificado de confianza.

3. Haga clic en **examinar** para seleccionar los archivos de certificado para los controladores.

Se muestran los nombres de los archivos en el cuadro de diálogo.

4. Haga clic en **Importar**.

Resultados

Los archivos se cargan y validan.

Habilite la comprobación de revocación de certificados

Es posible habilitar comprobaciones automáticas de certificados revocados para que el servidor de protocolo de estado de certificado en línea (OCSP) bloquee los usuarios y no permita que realicen conexiones no seguras.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Existe un servidor DNS configurado en las dos controladoras, lo que permite usar un nombre de dominio completo para el servidor OCSP. Esta tarea está disponible en la página hardware.
- Si desea especificar su propio servidor OCSP, debe conocer la URL de ese servidor.

Acerca de esta tarea

La comprobación de revocación automática es útil cuando la CA emite de manera incorrecta un certificado o cuando la clave privada está en riesgo.

Durante esta tarea, es posible configurar un servidor OCSP o usar el servidor especificado en el archivo de certificado. El servidor OCSP determina si la CA revocó algún certificado antes de su fecha de vencimiento

programada y, a continuación, bloquea al usuario para que no acceda al sitio si se ha revocado el certificado.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. Seleccione la ficha **Trusted**.



También puede habilitar la comprobación de revocación en la ficha **Gestión de claves**.

3. Haga clic en **tareas no comunes** y seleccione **Activar comprobación de revocación** en el menú desplegable.
4. Seleccione **deseo habilitar la comprobación de revocación**, de modo que aparezca una Marca de verificación en la casilla de verificación y aparecerán campos adicionales en el cuadro de diálogo.
5. En el campo **Dirección de respondedor OCSP**, puede especificar opcionalmente una URL para un servidor de respuesta OCSP. Si no se especifica ninguna dirección, el sistema utiliza la URL del servidor OCSP incluida en el archivo de certificado.
6. Haga clic en **Dirección de prueba** para asegurarse de que el sistema pueda abrir una conexión a la URL especificada.
7. Haga clic en **Guardar**.

Resultados

Si la cabina de almacenamiento intenta conectarse a un servidor que posee un certificado revocado, la conexión se rechaza y se registra un evento.

Elimine certificados de confianza

Es posible eliminar los certificados instalados por el usuario que se importaron anteriormente desde la pestaña de confianza.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Si actualiza a una nueva versión de certificado de confianza, el certificado actualizado debe importarse antes de eliminar el anterior.



Si elimina un certificado que se utiliza para autenticar las controladoras y otro servidor, como un servidor LDAP, antes de importar un certificado de reemplazo, puede perder el acceso al sistema.

Acerca de esta tarea

En esta tarea, se describe la manera de eliminar certificados instalados por el usuario. No se pueden eliminar los certificados autofirmados preinstalados.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. Seleccione la ficha **Trusted**.

En la tabla, se muestran los certificados de confianza de la cabina de almacenamiento.

3. En la tabla, seleccione el certificado que desea eliminar.

4. Haga clic en **menú:tareas no comunes[Eliminar]**

Se abrirá el cuadro de diálogo Confirmar eliminación de certificado de confianza.

5. Tipo `delete` En el campo y, a continuación, haga clic en **Eliminar**.

Use certificados firmados por CA para la autenticación con un servidor de gestión de claves

Para establecer comunicaciones seguras entre un servidor de gestión de claves y las controladoras de la cabina de almacenamiento, debe configurar los conjuntos de certificados adecuados.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Acerca de esta tarea

La autenticación entre las controladoras y un servidor de gestión de claves es un procedimiento de dos pasos.

Paso 1: Complete y envíe una CSR para la autenticación con un servidor de gestión de claves

Primero, debe generar un archivo de solicitud de firma de certificación (CSR) y utilizar la CSR para solicitar un certificado de cliente firmado de una entidad de certificación (CA) que confía en el servidor de gestión de claves. También es posible crear y descargar un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Acerca de esta tarea

En esta tarea, se describe cómo generar el archivo CSR, el cual se utilizará para solicitar un certificado de cliente firmado de una CA de confianza en el servidor de gestión de claves. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP). Durante esta tarea, debe brindar información acerca de su organización.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Gestión de claves**, seleccione **completar CSR**.
3. Introduzca la siguiente información:
 - **Nombre común** — un nombre que identifica a esta CSR, como el nombre de la matriz de almacenamiento, que se mostrará en los archivos de certificado.
 - **Organización** — el nombre completo y legal de su empresa u organización. Incluya sufijos, como Inc. O Corp
 - **Unidad organizativa (opcional)** — la división de su organización que maneja el certificado.
 - **Ciudad/localidad** — la ciudad o localidad donde está ubicada su organización.
 - **Estado/Región (opcional)** — el estado o región donde está ubicada su organización.
 - **Código ISO de país** — el código ISO (Organización Internacional de Normalización) de dos dígitos,

como US, en el que se encuentra su organización.

4. Haga clic en **Descargar**.

Se guardará un archivo CSR en el sistema local.

5. Solicite un certificado de cliente firmado de una CA a la que confíe el servidor de gestión de claves.

6. Cuando tenga un certificado de cliente, vaya a. [Paso 2: Importar certificados para el servidor de gestión de claves](#).

Paso 2: Importar certificados para el servidor de gestión de claves

Como paso siguiente, debe importar certificados para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves. Existen dos tipos de certificados: El certificado de cliente valida las controladoras de la cabina de almacenamiento, mientras que el certificado de servidor de gestión de claves valida al servidor.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Tiene un archivo de certificado de cliente firmado (consulte [Paso 1: Complete y envíe una CSR para la autenticación con un servidor de gestión de claves](#)), y copió ese archivo en el host donde se accede a System Manager. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP).
- Debe recuperar el archivo de certificado del servidor desde el servidor de gestión de claves y, a continuación, copiar ese archivo en el host donde se accede a System Manager. Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP.



Si desea obtener más información sobre el certificado de servidor, consulte la documentación del servidor de gestión de claves.

Acerca de esta tarea

En esta tarea, se describe cómo cargar archivos de certificado para la autenticación entre las controladoras de la cabina de almacenamiento y el servidor de gestión de claves. Debe cargar tanto el archivo de certificado de cliente para las controladoras como el archivo de certificado de servidor para el servidor de gestión de claves.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. En la ficha **Gestión de claves**, seleccione **Importar**.

Se abre un cuadro de diálogo para importar los archivos de certificado.

3. Junto a **Seleccionar certificado de cliente**, haga clic en el botón **examinar** para seleccionar el archivo de certificado de cliente para los controladores de la matriz de almacenamiento.

Se muestra el nombre del archivo en el cuadro de diálogo.

4. Junto a **Seleccionar certificado de servidor del servidor de administración de claves**, haga clic en el botón **examinar** para seleccionar el archivo de certificado de servidor del servidor de administración de claves.

Se muestra el nombre del archivo en el cuadro de diálogo.

5. Haga clic en **Importar**.

Los archivos se cargan y validan.

Exportar certificados del servidor de gestión de claves

Es posible guardar un certificado para un servidor de gestión de claves en una máquina local.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Los certificados deben haberse importado previamente.

Pasos

1. Seleccione **MENU:Settings[Certificates]**.
2. Seleccione la ficha **Gestión de claves**.
3. En la tabla, seleccione el certificado que desea exportar y, a continuación, haga clic en **Exportar**.

Se abre el cuadro de diálogo Guardar.

4. Introduzca un nombre de archivo y haga clic en **Guardar**.

Preguntas frecuentes

¿Por qué se muestra el cuadro de diálogo no se puede acceder a otra controladora?

Cuando se realizan ciertas operaciones relacionadas con los certificados de CA (por ejemplo, la importación de un certificado), es posible que aparezca un cuadro de diálogo que le solicite aceptar un certificado autofirmado para la segunda controladora.

En las cabinas de almacenamiento con dos controladoras (configuraciones dúplex), este cuadro de diálogo aparece en ocasiones si System Manager de SANtricity no puede comunicarse con la segunda controladora, o bien si el explorador no puede aceptar el certificado durante un determinado punto en una operación.

Si se abre este cuadro de diálogo, haga clic en **Aceptar certificado autofirmado** para continuar. Si otro cuadro de diálogo le solicita una contraseña, introduzca la contraseña de administrador que utiliza para acceder a System Manager.

En caso de que este cuadro de diálogo se muestre nuevamente y no pueda completar una tarea de certificado, intente uno de los procedimientos a continuación:

- Utilice un tipo de explorador diferente para acceder a esta controladora, acepte el certificado y continúe.
- Acceda a la segunda controladora con System Manager, acepte el certificado autofirmado y luego regrese a la primera controladora y continúe.

¿Cómo saber qué certificados deben cargarse en System Manager para la gestión de claves externas?

Para la gestión de claves externas, debe importar dos tipos de certificados para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves, de forma tal que exista confianza mutua entre las dos entidades.

Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP). Para obtener un certificado de cliente, se usa System Manager para completar una CSR para la cabina de almacenamiento. Luego, puede cargar la CSR en un servidor de gestión de claves y generar un certificado de cliente a partir de ese punto. Una vez que tenga un certificado de cliente, copie ese archivo en el host donde acceda a System Manager.

Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP. Recupere el archivo de certificado de servidor del servidor de gestión de claves y copie ese archivo en el host donde va a acceder a System Manager.

¿Qué debo saber acerca de la comprobación de revocación de certificados?

System Manager permite verificar certificados revocados mediante un servidor de protocolo de estado de certificado en línea (OCSP), en lugar de cargar listas de revocación de certificados (CRL).

Los certificados revocados ya no deberán considerarse de confianza. Un certificado puede ser revocado por varios motivos; por ejemplo, si la entidad de certificación (CA) emitió el certificado incorrectamente, una clave privada quedó en riesgo o la entidad identificada no cumplió con los requisitos de la política.

Después de establecer una conexión con un servidor OCSP en System Manager, la cabina de almacenamiento realiza la verificación de revocación cada vez que se conecta a un servidor de AutoSupport, un servidor de gestión de claves externo (EKMS), un servidor de protocolo ligero de acceso a directorios por SSL (LDAPS) o un servidor de syslog. La cabina de almacenamiento intenta validar los certificados de tales servidores para asegurarse de que no se hayan revocado. A continuación, el servidor obtiene los valores "good", "revoked" o "unknown" para ese certificado. Si el certificado se revoca o la cabina no puede conectarse al servidor de OCSP, la conexión se rechaza.



La especificación de una dirección de respuesta de OCSP en System Manager o en la interfaz de línea de comandos (CLI) anula la dirección de OCSP que se encontró en el archivo de certificado.

¿Para qué tipos de servidores se habilitará la comprobación de revocación?

La cabina de almacenamiento realiza la verificación de revocación cada vez que se conecta a un servidor AutoSupport, un servidor de gestión de claves externo (EKMS), un servidor de protocolo ligero de acceso a directorios por SSL (LDAPS) o un servidor de syslog.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.